IT - ITeS SSC NASSCOM

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

Qualification Pack

N·S·D·C National Skill Development Corporation
Transforming the skill landscape

Consultant Network Security

QP Code: SSC/Q0917

Version: 1.0

NSQF Level: 8

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

Contents

SSC/Q0917: Consultant Network Security

Brief Job Description

This job role is responsible for understanding network security needs from stakeholders and vulnerability analysis/penetration testing reports and researching and providing recommendations for solutions from existing network security solutions available. The consultant is also responsible for reviewing secure configuration and providing recommendations for minimum baseline security standards for all network security devices as well as for Network Security Policy and Standard operating procedures (SOPs).

Personal Attributes

This job may require the individual to work independently and take decisions for his/her own area of work. The individual should have a high level of analytical thinking ability, problem solving ability, passion for information security and attention for detail, should be ethical, compliance and result oriented, should also be able to demonstrate interpersonal and managerial skills.

Applicable National Occupational Standards (NOS)

Compulsory NOS:

1. SSC/N0918: Maintain compliance to information security policies, regulations and standards andaddress risk issues
2. SSC/N0922: Provide network security recommendations as per requirements
3. SSC/N0923: Carry out configuration review and provide recommendations for secure configuration of networks and security devices
4. SSC/N0925: Test, run exploits to identify vulnerabilities in networks
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 colleagues
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

Qualification Pack (QP) Parameters

Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information and Cyber Security
Country	India
NSQF Level	8
Aligned to NCO/ISCO/ISIC Code	NCO-2015/NIL
Minimum Educational Qualification & Experience	B.E./B.Tech (Security/ Computer Science/Electronics and Engineering/Information Technology) with 2-3 Years of experience Information technology
Minimum Level of Education for Training in School	12th Class
Pre-Requisite License or Training	NA
Minimum Job Entry Age	21 Years
Last Reviewed On	31/03/2018
Next Review Date	31/03/2022
NSQC Approval Date	19/12/2018
Version	1.0
Reference code on NQR	2019/ITES/ITSSC/03049
NQR Version	1.0

SSC/N0918: Maintain compliance to information security policies, regulations and standards andaddress risk issues

Description

This unit is about maintaining compliance to information security policies, regulations and standards and address risk issues in organizations.

Scope

This unit/task covers the following:Operating procedures include:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityCompliance audit and risk assessment:
- executive briefings
- risk assessment reports
- dashboardsProfessional and technical knowledge:
- by attending educational workshops
- reviewing professional publications
- establishing personal networks
- benchmarking state-of-the-art practices
- participating in professional societiesBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code like o viruso Trojano logic bombo wormo spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etc.

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. communicate the subsequent compliance audit and risk assessment results to specified organizational personnel

PC2. share compliance issues identified during the audit with appropriate organizational personnel as per process laid out

PC3. plan and coordinate the operational activities of a given company or organization to guarantee compliance with governmental regulations, ordinances and standards

PC4. ensure that all policies and procedures are implemented and well documented

PC5. perform occasional internal reviews, and identify compliance problems that call for formal attention

PC6. file compliance reports with regulatory bodies

PC7. take necessary actions for closure of the risk and nonconformance issues during the lifecycle

PC8. present compliance issues identified to the management for prioritizing, support risk mitigation plan

PC9. co-ordinate for ongoing monitoring of the risk factors to organizational operations and assets, individuals, other organizations

PC10. undertake corrective actions or implementation of controls or procedural steps for satisfying needs of compliances

PC11. implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service

PC12. maintain quality service by establishing and enforcing organization standards

PC13. maintain legal and regulatory compliance by researching and communicating requirements, and obtain approvals

PC14. maintain regular communication and contact with organizational head and other departments to share information and to ensure that compliance related activities are coordinated

PC15. document steps undertaken during the process & outcomes of the steps taken

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

PC17. complete research assignments and deliver comprehensive but concise reports in a timely manner

PC18. provide timely feedback on contracts and agreements to be issued or entered into by the organization

PC19. maintain professional and technical knowledge by formal and informal means

PC20. ensure that customer needs are met within SLA and meet other time and quality commitment KPIs

PC21. maintain a collaborative relationship with various stakeholders like management, other function heads and point of contacts, etc

PC22. provide guidance and suggestions as appropriate

PC23. complete own assigned tasks and activities to defined standards and timelines

PC24. correctly follow and apply the policies and standards relating to information security identity and access management activities

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. Organizational hierarchy and management structure

KU6. Legal and regulatory guidelines applicable to the business or domain that the organization is engaged in

KU7. how to engage with both internal and external specialists for support in order to resolve incidents and service requests

KU8. service request procedures, tools, and techniques

KU9. the operating procedures that are applicable to the system(s) being used

KU10. typical response times and service times related to own work area

KU11. computer network defense (CND) policies, procedures, and regulations

KU12. Basic cyber security concepts

KU13. explain how hardware and software vulnerabilities can be identified and resolved

KU14. what is meant by risk management, risk mitigation and risk control and what these entail

KU15. what are the aims and objectives of risk management

KU16. activities that are involved in the management of risk

KU17. the procedures, tools and techniques that can be used to conduct and document risk assessment activities

KU18. known vulnerabilities from alerts, advisories, errata, and bulletins

KU19. business objectives of the organization

KU20. the steps involved in information security risk management

KU21. compliance policies of the organization concerned

KU22. organizational procedures for information security audits

KU23. Risk Management Framework (RMF) requirements

KU24. information technology (IT) supply chain security/risk management policies, requirements, and procedures

KU25. various types of controls and safeguards for cyber security

KU26. computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities

KU27. systems diagnostic tools and fault identification techniques

KU28. new and emerging information technology (IT) and information security technologies

KU29. structured analysis principles and methods

KU30. names and uses of systems diagnostic tools and fault identification techniques

KU31. organizations enterprise information technology (IT) goals and objectives

KU32. relevant laws, policies, procedures, or standards as they relate to work that may impact critical infrastructure

KU33. Information Security concepts, policies, and procedures

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. document call logs, reports, task lists, and schedules with co-workers

GS2. prepare status and progress reports

GS3. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes

GS4. read about new products and services with reference to the organization and also from external forums such as websites and blogs

GS5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets

GS6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal

GS7. read policy manual, standard operating procedures and service level agreements relevant to work area

GS8. read emails received from own team, across team and external vendors and clients

GS9. discuss task lists, schedules, and work-loads with co-workers

GS10. give clear instructions to specialists/vendors/users/clients as required

GS11. keep stakeholders informed about progress

GS12. avoid using jargon, slang or acronyms when communicating with a customer,unless it is required

GS13. receive and make phone calls, including call forward, call hold, and call mute

GS14. follow rule-based decision-making processes

GS15. make decisions on suitable courses of action

GS16. plan and organize your work to achieve targets and deadlines

GS17. carry out rule-based transactions in line with customer-specific guidelines

GS18. procedures, rules and service level agreements

GS19. check your own and/or your peers work meets customer requirements

GS20. apply problem-solving approaches in different situations

GS21. seek clarification on problems from others

GS22. analyze data and activities

GS23. configure data and disseminate relevant information to others

GS24. pass on relevant information to others

GS25. provide opinions on work in a detailed and constructive way

GS26. apply balanced judgments to different situations

GS27. apply good attention to details

GS28. check your work is complete and free from errors

GS29. work effectively in a team environment

GS30. contribute to the quality of team working

GS31. work independently and collaboratively

GS32. determine how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes

GS33. identify measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system

GS34. evaluate the trustworthiness of the supplier and/or product

GS35. work on various operating systems

GS36. work with word processors, spreadsheets and presentations

GS37. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. communicate the subsequent compliance audit and risk assessment results to specified organizational personnel	1	3	-	-
PC2. share compliance issues identified during the audit with appropriate organizational personnel as per process laid out	1	3	-	-
PC3. plan and coordinate the operational activities of a given company or organization to guarantee compliance with governmental regulations, ordinances and standards	2	3	-	-
PC4. ensure that all policies and procedures are implemented and well documented	1	3	-	-
PC5. perform occasional internal reviews, and identify compliance problems that call for formal attention	2	3	-	-
PC6. file compliance reports with regulatory bodies	1	2	-	-
PC7. take necessary actions for closure of the risk and nonconformance issues during the lifecycle	2	3	-	-
PC8. present compliance issues identified to the management for prioritizing, support risk mitigation plan	2	3	-	-
PC9. co-ordinate for ongoing monitoring of the risk factors to organizational operations and assets, individuals, other organizations	1	4	-	-
PC10. undertake corrective actions or implementation of controls or procedural steps for satisfying needs of compliances	2	3	-	-
PC11. implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service	2	3	-	-
PC12. maintain quality service by establishing and enforcing organization standards	1	3	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC13. maintain legal and regulatory compliance by researching and communicating requirements, and obtain approvals	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	1	3	-	-
PC15. document steps undertaken during the process & outcomes of the steps taken	1	2	-	-
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	1	2	-	-
PC17. complete research assignments and deliver comprehensive but concise reports in a timely manner	2	3	-	-
PC18. provide timely feedback on contracts and agreements to be issued or entered into by the organization	1	3	-	-
PC19. maintain professional and technical knowledge by formal and informal means	1	3	-	-
PC20. ensure that customer needs are met within SLA and meet other time and quality commitment KPIs	1	2	-	-
PC21. maintain a collaborative relationship with various stakeholders like management, other function heads and point of contacts, etc	1	3	-	-
PC22. provide guidance and suggestions as appropriate	2	2	-	-
PC23. complete own assigned tasks and activities to defined standards and timelines	1	3	-	-
PC24. correctly follow and apply the policies and standards relating to information security identity and access management activities	1	3	-	-
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0918
NOS Name	Maintain compliance to information security policies, regulations and standards andaddress risk issues
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	7
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0922: Provide network security recommendations as per requirements

Description

This unit is about identifying needs, researching and recommending network security solutions as per requirements.

Scope

This unit/task covers the following:Operating procedures includes:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentiality Network security measures are:
- firewall, to keep unauthorized users off the network
- virtual private network (VPN), to give employees, customers, and partners secure access to the network
- intrusion prevention, to detect and stop threats before they harm the network
- content security, to protect the network from viruses, spam, spyware, and other attacks
- secure wireless network, to provide safe network access to visitors and employees on the go
- identity management, to give the business owner control over who and what can access the network
- compliance validation, to make sure that any device accessing the network
- meets the security requirement deep packet inspectionBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code likeo viruso Trojano logic bombo wormo spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etcRelevant networking concepts, devices and terminology such as:
- Concepts: OSI Model/topology; Network Protocols, bandwidth management, etc.
- Devices and databases: Switches, routers, Intrusion detection and prevention System (IDPS), etc.
- Terminology: SSL, VPN, 2FA, Encryption, IPSEC, TLS, IP subnetting, network routing, RADIUS, TACACS+etc.Tools and technologies used in network security include but are not limited to:
- IP Scanners
- Sniffers
- Bandwidth Monitoring
- Network Monitoring tool
- Packet analyser
- Computer network defence (CND)Security principles and methods are:
- firewalls
- demilitarized zones

- encryption

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. consult with customers to evaluate functional requirements for network security

PC2. define project scope and objectives based on customer requirements

PC3. confirm availability of complete and accurate details of the security objectives

PC4. Evaluate the existing network protocols and topology of users

PC5. review the usage of existing network security measures, and assess risks w.r.t security objectives

PC6. consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements

PC7. conduct technical risk analysis, threat identification of the existing network security measures

PC8. identify level of risk acceptable for business requirements by discussing with business and technical leads

PC9. critically interpret information and data, from both within the customer/client organisation and other sources, in order to identify network security requirements

PC10. research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks

PC11. identify and record details of constraints that may have an impact on the business and security options

PC12. explore potential vulnerabilities that could be technical, operational or management related

PC13. categorize vulnerabilities and identify extent of vulnerability including level of weakness and sensitivity of the information

PC14. identify the root cause of vulnerabilities

PC15. research options of network security solutions that match the and security requirements captured

PC16. gather sufficient accurate information on which to determine potential costs, benefits and effectiveness of potential security solutions

PC17. identify and determine the cost, potential benefits, and effectiveness of recommended security solutions, based on valid assumptions, considerations and information, including possible constraints

PC18. prepare recommendations that have the potential to meet the security objectives of the organisation

PC19. provide details of costs, benefits, effectiveness, limitations and constraints of recommendations

PC20. provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales

PC21. provide the organisation with considered advice on the implications of accepting, modifying or rejecting security recommendations

PC22. co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs

PC23. take account of the organisations values, culture and nature of business
PC24. maintain the security and confidentiality of information relating to your organisation and recommendations
PC25. obtain necessary approvals from the responsible persons as per organisational policy
PC26. evaluate ways & means of closing weaknesses in the network
PC27. maintain logs for all the activities performed

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company
KU2. organizations knowledge base and how to access and update this
KU3. limits of your role and responsibilities and who to seek guidance from
KU4. he organizational systems, procedures and tasks/checklists within the domain and how to use these
KU5. the operating procedures that are applicable to the system(s) being used
KU6. typical response times and service times related to own work area
KU7. standard tools and templates available and how to use these
KU8. basic cyber security concepts
KU9. how hardware and software vulnerabilities can be identified and resolved
KU10. relevant networking concepts, devices and terminology
KU11. network security principles and processes
KU12. network security tools, technologies and applications
KU13. vulnerability analysis and penetration testing report templates
KU14. various sources for researching for existing network security solution
KU15. categorization and root cause analysis process of vulnerabilities
KU16. types of addresses used on networks and why they are used
KU17. basics of enterprise information technology (IT) architecture Information Technology Architecture
KU18. extension points of the products (for customization and integration with other applications)
KU19. secure integration approach with different third party systems
KU20. statutory knowledge (IT Act, TRAI Guidelines, and other national and international Guidelines)
KU21. standards and industry best practices for network security
KU22. new technological developments in Network security
KU23. principles and methods for integrating technology components
KU24. traffic analysis using flow and pcaps
KU25. server administration and systems engineering theories, concepts, and methods Systems Life Cycle
KU26. Segregation of Duties (SoD) configuration
KU27. migration of systems and users

KU28. the basic functionalities of the applications, hardware and/or access rights that are used by the customers

KU29. host/network access controls (e.g., access control list)

KU30. Advanced knowledge of cloud security

KU31. intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate well written work with attention to detail

GS2. document call logs, reports, task lists, and schedules with co-workers

GS3. prepare status and progress reports

GS4. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes

GS5. write standard operating procedures (SOPs) and reports relevant to work area

GS6. read about new products and services with reference to the organization and also from external forums such as websites and blogs

GS7. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets

GS8. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal

GS9. read policy manual, standard operating procedures and service level agreements relevant to work area

GS10. read emails received from own team, across team and external vendors and clients

GS11. discuss task lists, schedules, and work-loads with co-workers

GS12. solicit and record information by asking pertinent questions from various stakeholders

GS13. give clear instructions to specialists/vendors/users/clients as required

GS14. make presentations to stakeholders

GS15. keep stakeholders informed about progress through MIS reports

GS16. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required

GS17. receive and make phone calls, including call forward, call hold, and call mute

GS18. follow rule-based decision-making processes

GS19. make a decision on a suitable course of action

GS20. plan and organize your work to achieve targets and deadlines

GS21. Identify internal or external customer requirement and priorities clearly with respect to work at hand

GS22. carry out rule-based transactions in line with customer-specific guidelines, procedures, rules and service level agreements

GS23. check that your own and/or your peers work meets customer requirements

GS24. apply problem-solving approaches in different situations
GS25. seek clarification on problems from others
GS26. analyze data and activities
GS27. configure data and disseminate relevant information to others
GS28. pass on relevant information to others
GS29. provide opinions on work in a detailed and constructive way
GS30. apply balanced judgments to different situations
GS31. check your work is complete and free from errors
GS32. work effectively in a team environment
GS33. work independently and collaboratively
GS34. configure, diagnose and troubleshoot computer networks using in-depth understanding of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], HTTPS, SSH, FTP, Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])
GS35. administer, use and monitor of an intrusion detection system
GS36. Install and configure firewalls, routers, Intrusion detection and prevention System(IDPS)
GS37. read and write coded scripts and modify and debug programs
GS38. collect data from a variety of computer network defense resources
GS39. work on various operating system
GS40. work with word processers, spreadsheets and presentations
GS41. perform basic penetration testing and ethical hacking
GS42. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. consult with customers to evaluate functional requirements for network security	1	3	-	-
PC2. define project scope and objectives based on customer requirements	1	3	-	-
PC3. confirm availability of complete and accurate details of the security objectives	1	2	-	-
PC4. Evaluate the existing network protocols and topology of users	2	2	-	-
PC5. review the usage of existing network security measures, and assess risks w.r.t security objectives	2	2	-	-
PC6. consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements	1	3	-	-
PC7. conduct technical risk analysis, threat identification of the existing network security measures	2	3	-	-
PC8. identify level of risk acceptable for business requirements by discussing with business and technical leads	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	1	3	-	-
PC10. research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks	1	3	-	-
PC11. identify and record details of constraints that may have an impact on the business and security options	1	2	-	-
PC12. explore potential vulnerabilities that could be technical, operational or management related	2	3	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC13. categorize vulnerabilities and identify extent of vulnerability including level of weakness and sensitivity of the information	2	2	-	-
PC14. identify the root cause of vulnerabilities	1	3	-	-
PC15. research options of network security solutions that match the and security requirements captured	1	4	-	-
PC16. gather sufficient accurate information on which to determine potential costs, benefits and effectiveness of potential security solutions	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	1	2	-	-
PC18. prepare recommendations that have the potential to meet the security objectives of the organisation	1	3	-	-
PC19. provide details of costs, benefits, effectiveness, limitations and constraints of recommendations	1	2	-	-
PC20. provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales	1	2	-	-
PC21. provide the organisation with considered advice on the implications of accepting, modifying or rejecting security recommendations	1	2	-	-
PC22. co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs	1	3	-	-
PC23. take account of the organisations values, culture and nature of business	1	2	-	-
PC24. maintain the security and confidentiality of information relating to your organisation and recommendations	1	2	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC25. obtain necessary approvals from the responsible persons as per organisational policy	1	2	-	-
PC26. evaluate ways & means of closing weaknesses in the network	1	3	-	-
PC27. maintain logs for all the activities performed	1	2	-	-
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0922
NOS Name	Provide network security recommendations as per requirements
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0923: Carry out configuration review and provide recommendations for secure configuration of networks and security devices

Description

This unit is about carrying out configuration review and providing recommendations for secure configuration of networks and security devices.

Scope

This unit/task covers the following:Various means of protecting configuration files include but are not limited to:

- encode and Encrypt and/or a salted hash with iteration to protect confidentiality of passwords in configuration files
- change passwords/keys immediately if the network device configuration file is transmitted in the clear (or is otherwise exposed) while containing non-encrypted passwords/keys Operating procedures includes:
- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code likeo viruso Trojano logic bombo wormo spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etc.Relevant networking concepts, devices and terminology such as:
- Concepts: OSI Model/topology; Network Protocols, bandwidth management, etc.
- Devices and databases: Switches, routers, Intrusion detection and prevention System (IDPS), etc.
- Terminology: SSL, VPN, 2FA, Encryption, IPSEC, TLS, IP subnetting, network routing, RADIUS, TACACS+etc.Security principles and methods are:
- firewalls
- demilitarized zones
- encryption

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. conduct an inventory to identify the network configuration items that need to be secured

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

PC3. identify and record the configurations of network configuration items that impact the cyber security posture of the organization

PC4. review initial configuration of network configuration items considering security vulnerabilities and threats identified

PC5. provide recommendations for secure configuration measures for networks considering business requirements

PC6. establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements

PC7. provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of the organization and business requirements

PC8. provide recommendation of appropriate solution for secure configuration management (SCM solution) as per requirements of the organisation

PC9. test secure configurations prior to implementation in the production environment

PC10. diagnose issues and respond to queries from the implementation team with respect to various secure configuration processes and specifications

PC11. suggest remediation actions to resolve issues caused due to erroneous network device configurations

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. the operating procedures that are applicable to the system(s) being used

KU6. typical response times and service times related to own work area

KU7. standard tools and templates available and how to use these

KU8. basic cyber security concepts

KU9. how hardware and software vulnerabilities can be identified and resolved

KU10. relevant networking concepts, devices and terminology

KU11. how to install, integrate, and optimize system components

KU12. information technology (IT) security principles and methods

KU13. network access, identity and access management

KU14. network design processes, to include understanding of security objectives, operational objectives, and tradeoffs

KU15. network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools

KU16. network traffic analysis methods

KU17. importance of secure configuration management of network devices
KU18. secure configuration management activities
KU19. secure configuration measures and process for network devices
KU20. patch Management and malware protection
KU21. available secure configuration management (SCM) solutions
KU22. system development life cycle (SDLC)
KU23. baseline configuration
KU24. process for testing the network to ascertain that it has not been breached
KU25. traffic filtering technologies and the needs they fulfill
KU26. various means of protecting configuration files
KU27. what could be sensitive data and transaction flows in an organization
KU28. process for scanning an organizations Internet address ranges
KU29. windows command line (e.g., ipconfig, netstat, dir, nbtstat)
KU30. unix command line (e.g., mkdir, mv, ls, passwd, grep)
KU31. common attack vectors on the network layer

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate well written work with attention to detail
GS2. document call logs, reports, task lists, and schedules with co-workers
GS3. Prepare status and progress reports
GS4. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes
GS5. read about new products and services with reference to the organization and also from external forums such as websites and blogs
GS6. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets
GS7. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal
GS8. read policy manual, standard operating procedures and service level agreements relevant to work area
GS9. read emails received from own team, across team and external vendors and clients
GS10. discuss task lists, schedules, and work-loads with co-workers
GS11. give clear instructions to specialists/vendors/users/clients as required
GS12. keep stakeholders informed about progress
GS13. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required
GS14. receive and make phone calls, including call forward, call hold, and call mute
GS15. follow rule-based decision-making processes

GS16. make a decision on a suitable course of action

GS17. plan and organize your work to achieve targets and deadlines

GS18. Identify internal or external customer requirement and priorities clearly with respect to work at hand

GS19. carry out rule-based transactions in line with customer-specific guidelines, procedures, rules and service level agreements

GS20. check that your own and/or your peers work meets customer requirements

GS21. apply problem-solving approaches in different situations

GS22. seek clarification on problems from others

GS23. analyze data and activities

GS24. configure data and disseminate relevant information to others

GS25. pass on relevant information to others

GS26. provide opinions on work in a detailed and constructive way

GS27. apply balanced judgments to different situations

GS28. check your work is complete and free from errors

GS29. work effectively in a team environment

GS30. work effectively in a team environment

GS31. configure, diagnose and troubleshoot computer networks using in-depth understanding of TCP/IP protocols

GS32. update firewall IP address and subnet masks

GS33. change default username and passwords of the firewall devices

GS34. administer, use and monitor of an intrusion detection system

GS35. configure firewalls and routers

GS36. update firewall IP address and subnet masks

GS37. change default username and passwords of the firewall devices

GS38. work on various operating system

GS39. work with word processers, spreadsheets and presentations

GS40. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. conduct an inventory to identify the network configuration items that need to be secured	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	3	6	-	-
PC3. identify and record the configurations of network configuration items that impact the cyber security posture of the organization	3	5	-	-
PC4. review initial configuration of network configuration items considering security vulnerabilities and threats identified	3	5	-	-
PC5. provide recommendations for secure configuration measures for networks considering business requirements	3	6	-	-
PC6. establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements	3	6	-	-
PC7. provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of the organization and business requirements	3	6	-	-
PC8. provide recommendation of appropriate solution for secure configuration management (SCM solution) as per requirements of the organisation	3	6	-	-
PC9. test secure configurations prior to implementation in the production environment	4	7	-	-
PC10. diagnose issues and respond to queries from the implementation team with respect to various secure configuration processes and specifications	3	7	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC11. suggest remediation actions to resolve issues caused due to erroneous network device configurations	2	8	-	-
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0923
NOS Name	Carry out configuration review and provide recommendations for secure configuration of networks and security devices
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0925: Test, run exploits to identify vulnerabilities in networks

Description

This unit is about performing network vulnerability assessment.

Scope

This unit/task covers the following:Operating procedures includes:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityPreliminary Information:
- scope and schedule of work
- type of assessment
- business priorities
- type of network and network components
- constraints
- already identified risks and vulnerabilities
- possible areas of weakness Information gathering tools:
- IP Scanners
- Sniffers
- Bandwidth Monitoring
- Network Monitoring tool
- packet analyser
- computer network defence (CND)sInformation gathering methods:
- conduct Search Engine Discovery and Reconnaissance for Information Leakage
- Create IP schema for all network security devices, update quarterly Active Reconnaissance:
- touching the target(network) directly Public repositories are:
- whois databases
- domain registrars
- usenet groups
- mailing lists Pivoting techniques:
- Pivoting is a process in which a penetration tester uses the compromised (target) system to attack other systems in the target network. Basic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code likeo virus o Trojan o logic bomb o worm o spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etc.Relevant networking concepts, devices and terminology such as:
- Concepts: OSI Model/topology; Network Protocols, bandwidth management, host network access

controls, directory services, etc.
- Devices: Hubs, switches, routers, bridges, servers, transmission media, Intrusion detection and prevention System(IDPS), etc.
- Databases: Oracle, SQL, MySQL
- Terminology: SSL, VPN, 2FA, Encryption, IPSEC, TLS, IP subnetting, network routing, RADIUS, TACACS+, etc. Encryption algorithms are:
- Internet Protocol Security [IPSEC]
- Advanced Encryption Standard [AES]
- Generic Routing Encapsulation [GRE]
- Internet Key Exchange [IKE]
- Message Digest Algorithm [MD5]
- Secure Hash Algorithm [SHA]
- Triple Data Encryption Standard [3DES] Security principles and methods are:
- firewalls
- demilitarized zones
- encryption Traffic flows are:
- Transmission Control Protocol and Internet Protocol [TCP/IP]
- Open System Interconnection model [OSI]
- Information Technology Infrastructure Library
- v3 [ITIL]) Network protocols are:
- Transmission Control Protocol and Internet Protocol [TCP/IP]
- Dynamic Host Configuration Protocol [DHCP]) Directory Services are:
- Domain Name System [DNS] Windows command line
- ipconfig
- netstat
- dir
- nbtstatUnix command line
- mkdir
- mv
- ls
- passwd
- grep

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. Consult with customers to evaluate functional requirements for network security.

PC2. Define project scope and objectives based on customer requirements.

PC3. Confirm the availability of complete and accurate details of the security objectives.

PC4. Review the usage of existing network security measures, and assess risks w.r.t security objectives.

PC5. create documents using standard templates and agreed language standards

PC6. Consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements.

PC7. Conduct technical risk analysis, threat identification of the existing network security measures

PC8. Identify the level of risk acceptable for business requirements by discussing with business and technical leads

PC9. Critically interpret information and data, from both within the customer/client organization and other sources, in order to identify network security requirements.

PC10. Research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks

PC11. Identify and record details of constraints that may have an impact on the business and security options.

PC12. Explore potential vulnerabilities that could be technical, operational or management related .

PC13. Categorize vulnerabilities and identify the extent of vulnerability including the level of weakness and sensitivity of the information .

PC14. Identify the root cause of vulnerabilities.

PC15. Research options of network security solutions that match the productivity and security requirements captured .

PC16. Gather sufficient accurate information on which to determine potential costs, benefits , and effectiveness of potential security solutions .

PC17. Identify and determine the cost, potential benefits, and effectiveness of recommended security solutions, based on valid assumptions, considerations , and information, including possible constraints .

PC18. Prepare recommendations that have the potential to meet the security objectives of the organization.

PC19. Provide details of costs, benefits, effectiveness, limitations , and constraints of recommendations

PC20. Provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales .

PC21. Provide the organization with considered advice on the implications of accepting, modifying or rejecting security recommendations .

PC22. Co ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs .

PC23. Take account of the organizations values, culture , and nature of the business .

PC24. Maintain the security and confidentiality of information relating to your organization and recommendations.

PC25. Obtain necessary approvals from the responsible persons as per organizational policy.

PC26. Evaluate ways & means of closing weaknesses in the network.

PC27. Maintain logs for all the activities performed

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. organizations knowledge base and how to access and update this

KU2. limits of your role and responsibilities and who to seek guidance from

KU3. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU4. the operating procedures that are applicable to the system(s) being used
KU5. typical response times and service times related to own work area
KU6. standard tools and templates available and how to use these
KU7. basic cyber security concepts
KU8. explain how hardware and software vulnerabilities can be identified and resolved
KU9. relevant networking concepts, devices and terminology
KU10. known vulnerabilities from alerts, advisories, errata, and bulletins
KU11. encryption algorithms
KU12. information technology (IT) security principles and methods
KU13. network access, identity, and access management
KU14. network design processes, to include understanding of security objectives, operational objectives, and tradeoffs
KU15. operating systems
KU16. how traffic flows across the network
KU17. parallel and distributed computing concepts
KU18. systems testing and evaluation methods
KU19. vulnerability assessment tools, including open source tools, and their capabilities
KU20. host/network access controls (e.g., access control list)
KU21. intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies
KU22. network traffic analysis methods
KU23. what constitutes a network attack and the relationship to both threats and vulnerabilities
KU24. Various types of network security devices, their roles and hardening requirements
KU25. standard System Development Life Cycle (SDLC) practices and process
KU26. patch management and its importance
KU27. importance of regular operation and maintenance on network security devices and what does it include
KU28. windows command line
KU29. unix command line
KU30. the common attack vectors on the network layer
KU31. internet ports, protocols and services and their usefulness
KU32. security solutions like Firewall, Intrusion detection and prevention System (IDPS), web security gateways, email security, content management, etc.
KU33. new technological developments in network security
KU34. basics of mobile network security and cloud network security
KU35. key features of mobile and cloud network testing tools

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate well written work with attention to detail

GS2. document call logs, reports, task lists, and schedules with co-workers

GS3. prepare status and progress reports

GS4. log calls and raise tickets in the SIEM tool, providing proper indicators and descriptions as required

GS5. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes

GS6. read about new products and services with reference to the organization and also from external forums such as websites and blogs

GS7. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets

GS8. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal

GS9. read policy manual, standard operating procedures and service level agreements relevant to work area

GS10. read emails received from own team, across team and external vendors and clients

GS11. discuss task lists, schedules, and work-loads with co-workers

GS12. give clear instructions to specialists/vendors/users/clients as required

GS13. keep stakeholders informed about progress

GS14. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required

GS15. receive and make phone calls, including call forward, call hold, and call mute

GS16. follow rule-based decision-making processes

GS17. make a decision on a suitable course of action

GS18. plan and organize your work to achieve targets and deadlines

GS19. Identify internal or external customer requirement and priorities clearly with respect to work at hand

GS20. carry out rule-based transactions in line with customer-specific guidelines, procedures, rules and service level agreements

GS21. check that your own and/or your peers work meets customer requirements

GS22. apply problem-solving approaches in different situations

GS23. seek clarification on problems from others

GS24. analyze data and activities

GS25. configure data and disseminate relevant information to others

GS26. pass on relevant information to others

GS27. provide opinions on work in a detailed and constructive way

GS28. apply balanced judgments to different situations

GS29. check your work is complete and free from errors

GS30. work effectively in a team environment

GS31. work independently and collaboratively

GS32. assess the robustness of security systems and designs

GS33. evaluate the adequacy of security designs

GS34. use network analysis tools to identify vulnerabilities

GS35. develop and deploy signatures custom tools/scripts with the help of various scripting languages like ShellScript, Python, Perl or Ruby and write exploits using programming languages like C

GS36. collect data from a variety of computer network defense resources

GS37. work on various operating system

GS38. work with word processers, spreadsheets and presentations

GS39. perform basic penetration testing and ethical hacking

GS40. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	30	**70**	**-**	**-**
PC1. Consult with customers to evaluate functional requirements for network security.	1	3	-	-
PC2. Define project scope and objectives based on customer requirements.	1	3	-	-
PC3. Confirm the availability of complete and accurate details of the security objectives.	1	2	-	-
PC4. Review the usage of existing network security measures, and assess risks w.r.t security objectives.	2	2	-	-
PC5. create documents using standard templates and agreed language standards	2	2	-	-
PC6. Consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements.	1	3	-	-
PC7. Conduct technical risk analysis, threat identification of the existing network security measures	2	3	-	-
PC8. Identify the level of risk acceptable for business requirements by discussing with business and technical leads	1	3	-	-
PC9. Critically interpret information and data, from both within the customer/client organization and other sources, in order to identify network security requirements.	1	3	-	-
PC10. Research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks	1	3	-	-
PC11. Identify and record details of constraints that may have an impact on the business and security options.	1	2	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC12. Explore potential vulnerabilities that could be technical, operational or management related .	1	4	-	-
PC13. Categorize vulnerabilities and identify the extent of vulnerability including the level of weakness and sensitivity of the information .	1	3	-	-
PC14. Identify the root cause of vulnerabilities.	1	3	-	-
PC15. Research options of network security solutions that match the productivity and security requirements captured .	1	4	-	-
PC16. Gather sufficient accurate information on which to determine potential costs, benefits , and effectiveness of potential security solutions .	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 .	1	2	-	-
PC18. Prepare recommendations that have the potential to meet the security objectives of the organization.	1	3	-	-
PC19. Provide details of costs, benefits, effectiveness, limitations , and constraints of recommendations	1	2	-	-
PC20. Provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales .	1	2	-	-
PC21. Provide the organization with considered advice on the implications of accepting, modifying or rejecting security recommendations .	1	2	-	-
PC22. Co ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs .	1	3	-	-
PC23. Take account of the organizations values, culture , and nature of the business .	1	2	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC24. Maintain the security and confidentiality of information relating to your organization and recommendations.	1	2	-	-
PC25. Obtain necessary approvals from the responsible persons as per organizational policy.	1	2	-	-
PC26. Evaluate ways & means of closing weaknesses in the network.	1	3	-	-
PC27. Maintain logs for all the activities performed	1	2	-	-
NOS Total	**30**	**70**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0925
NOS Name	Test, run exploits to identify vulnerabilities in networks
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	7
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0927: Drive interrelated cyber security actions

Description

This unit is about working with different teams to drive interrelated cyber security actions.

Scope

This unit/task covers the following:Cyber security functions and operations:

- vulnerability scanning
- threat management
- security monitoring and incident management
- security governance
- risk and compliance management
- security policy management
- security review and audit
- application security
- access and identity management
- endpoint securityKey Cyber security activities are: e.g.
- vulnerability scanning
- threat management
- security monitoring and incident management
- security governance
- risk and compliance management
- security policy management
- security review and audit
- application security
- access and identity management
- endpoint security, etc.Operating procedures include:
- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for informationsystems;
- common types of malicious code like o virus o Trojan o logic bomb o worm o spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability andmotive, etc.Security solutions:
- Firewall
- IDS/IPS
- web security gateways

- email security
- content management

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. identify the business functions, and key stakeholders within these, and establish their interest and understanding, relevant to achieving the organisation's aims

PC2. recognise the roles, responsibilities, interests and concerns of the stakeholders in other business functions

PC3. identify all the activities, functions and operations that are attributed to security or require analysis from security perspective

PC4. create an inventory of roles that are responsible, accountable and informed for activities, functions and operations in cyber security

PC5. create an inventory of cyber security operations that fall into various key cyber security activities

PC6. identify functions that have a joint working relationship with own function

PC7. consider implication of own work on other functions

PC8. discuss and consult with stakeholders from other functions in relation to key decisions and activities impacting them

PC9. take agreements and track actionables of other functions for interrelated work

PC10. follow up with appropriate personnel for meeting timelines and effective functioning

PC11. agree on communication and documentation process with stakeholders and maintain the same

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

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

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

PC15. undertake actions agreed with stakeholders in line with the terms of any agreements made

PC16. advise stakeholders of difficulties or where it will be impossible to fulfil agreed actions in line with the terms of any agreements made

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company including cyber security policy

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. the operating procedures that are applicable to the system(s) being used

KU6. typical response times and service times related to own work area

KU7. different business functions and their roles and responsibilities in achieving the organizations overall aims function

KU8. basic cyber security concepts

KU9. information assurance (IA) principles

KU10. various cyber security functions and operations

KU11. cyber security roles and responsibilities

KU12. the enterprise information technology (IT) architecture Information technology architecture

KU13. measures or indicators of system performance and availability Information

KU14. functions that can be impacted by own work

KU15. activities that will need joint working

KU16. various stakeholders to own work in other functions

KU17. internet ports, protocols and services and their usefulness

KU18. security solutions

KU19. the reasons why there may be conflicts and misunderstandings between business functions, for example, regarding which publics/stakeholders and activities are the most important

KU20. why it is important to identify key colleagues and stakeholders within the different business functions

KU21. principles of effective communication and how to apply them in order tocommunicate effectively with colleagues and stakeholders

KU22. why it is important to recognize the roles, responsibilities, interests and concerns of colleagues and stakeholders

KU23. how to consult with colleagues and stakeholders in relation to key decisions and activities

KU24. importance of taking account of the views of colleagues and stakeholders, particularly in relation to their priorities, expectations and attitudes towards the role of the marketing

KU25. why communication with colleagues and stakeholders on fulfilment of agreements or any problems affecting or preventing fulfilment is important

KU26. how to identify conflicts of interest with colleagues and stakeholders and the techniques that can be used to manage or remove them

KU27. importance of agreeing upon communication and documentation strategy for joint working

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. document call logs, reports, task lists, and schedules with co-workers

GS2. prepare status and progress reports

GS3. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes

GS4. read about new products and services with reference to the organization and also from external forums such as websites and blogs

GS5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets

GS6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal

GS7. read policy manual, standard operating procedures and service level agreements relevant to work area

GS8. read emails received from own team, across team and external vendors and clients

GS9. discuss task lists, schedules, and work-loads with co-workers

GS10. give clear instructions to specialists/vendors/users/clients as required

GS11. keep stakeholders informed about progress

GS12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required

GS13. receive and make phone calls, including call forward, call hold, and call mute

GS14. follow rule-based decision-making processes

GS15. make decisions on suitable courses of action

GS16. plan and organize your work to achieve targets and deadlines

GS17. carry out rule-based transactions in line with customer-specific guidelines,

GS18. procedures, rules and service level agreements

GS19. check your own and/or your peers work meets customer requirements

GS20. apply problem-solving approaches in different situations

GS21. seek clarification on problems from others

GS22. analyze data and activities

GS23. configure data and disseminate relevant information to others

GS24. pass on relevant information to others

GS25. provide opinions on work in a detailed and constructive way

GS26. apply balanced judgments to different situations

GS27. apply good attention to details

GS28. check your work is complete and free from errors

GS29. work effectively in a team environment

GS30. contribute to the quality of team working

GS31. work independently and collaboratively

GS32. work on various operating systems

GS33. work with word processors, spreadsheets and presentations

GS34. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

GS35. track deliverables and follow up with stakeholders

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	35	**65**	**-**	**-**
PC1. identify the business functions, and key stakeholders within these, and establish their interest and understanding, relevant to achieving the organisation's aims	-	4	-	-
PC2. recognise the roles, responsibilities, interests and concerns of the stakeholders in other business functions	3	3	-	-
PC3. identify all the activities, functions and operations that are attributed to security or require analysis from security perspective	-	4	-	-
PC4. create an inventory of roles that are responsible, accountable and informed for activities, functions and operations in cyber security	3	4	-	-
PC5. create an inventory of cyber security operations that fall into various key cyber security activities	3	4	-	-
PC6. identify functions that have a joint working relationship with own function	-	4	-	-
PC7. consider implication of own work on other functions	2	5	-	-
PC8. discuss and consult with stakeholders from other functions in relation to key decisions and activities impacting them	2	5	-	-
PC9. take agreements and track actionables of other functions for interrelated work	3	4	-	-
PC10. follow up with appropriate personnel for meeting timelines and effective functioning	3	5	-	-
PC11. agree on communication and documentation process with stakeholders and maintain the same	3	3	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
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	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	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	2	5	-	-
PC15. undertake actions agreed with stakeholders in line with the terms of any agreements made	3	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	3	4	-	-
NOS Total	**35**	**65**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0927
NOS Name	Drive interrelated cyber security actions
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information and Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0928: Manage a project team

Description

This unit is about managing a team working on a project.

Scope

This unit/task covers the following:Operating procedures includes:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentiality

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives

PC2. brief team members on the project and their work allocations

PC3. inform team members of changes to work allocations in an appropriate way

PC4. provide appropriate support and guidance to team members

PC5. monitor and assess the performance of the team against agreed objectives and work plans

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

PC7. take effective action to manage any actual or potential conflict between team members

PC8. update objectives and work plans regularly, to take account of any individual, team and organisational changes

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. the operating procedures that are applicable to the system(s) being used
KU6. typical response times and service times related to own work area
KU7. relevant legislative, regulatory and organizational requirements
KU8. the context of the project
KU9. the arrangements for the delivery of the project
KU10. relevant management plans for the project team
KU11. methods for monitoring and evaluating progress
KU12. how to allocate and authorize project work
KU13. how to communicate team and individual responsibilities clearly to those involved
KU14. how to manage conflict between team members
KU15. the application of negotiation and influencing skills
KU16. the differences between managing individuals for whom you have
KU17. managerial responsibility and those who you do not, and the implications this difference may have for project management

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. document call logs, reports, task lists, and schedules with co-workers
GS2. prepare status and progress reports
GS3. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes
GS4. read about new products and services with reference to the organization and also from external forums such as websites and blogs
GS5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets
GS6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal
GS7. read policy manual, standard operating procedures and service level agreements relevant to work area
GS8. read emails received from own team, across team and external vendors and clients
GS9. discuss task lists, schedules, and work-loads with co-workers
GS10. give clear instructions to specialists/vendors/users/clients as required
GS11. keep stakeholders informed about progress
GS12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required
GS13. receive and make phone calls, including call forward, call hold, and call mute
GS14. follow rule-based decision-making processes
GS15. make a decision on a suitable course of action
GS16. plan and organize your work to achieve targets and deadlines

GS17. carry out rule-based transactions in line with customer-specific guidelines,
GS18. procedures, rules and service level agreements
GS19. check your own and/or your peers work meets customer requirements
GS20. apply problem-solving approaches in different situations
GS21. seek clarification on problems from others
GS22. analyze data and activities
GS23. configure data and disseminate relevant information to others
GS24. pass on relevant information to others
GS25. provide opinions on work in a detailed and constructive way
GS26. apply balanced judgments to different situations
GS27. use information technology effectively, to make tracker, charts and reports
GS28. Use various modes of communication which working with the project team including but not limited to conference calls, group messaging, web conferences, video conferences, group sharing and working on documents on cloud, etc.
GS29. keep up to date with changes, procedures and practices in your role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives	3	9	-	-
PC2. brief team members on the project and their work allocations	3	9	-	-
PC3. inform team members of changes to work allocations in an appropriate way	3	9	-	-
PC4. provide appropriate support and guidance to team members	5	9	-	-
PC5. monitor and assess the performance of the team against agreed objectives and work plans	5	8	-	-
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	4	8	-	-
PC7. take effective action to manage any actual or potential conflict between team members	4	8	-	-
PC8. update objectives and work plans regularly, to take account of any individual, team and organisational changes	5	8	-	-
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0928
NOS Name	Manage a project team
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N9001: Manage your work to meet requirements

Description

This unit is about planning and organizing your work in order to complete it to the required standards on time.

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. establish and agree your work requirements with appropriate people
PC2. keep your immediate work area clean and tidy
PC3. utilize your time effectively
PC4. use resources correctly and efficiently
PC5. treat confidential information correctly
PC6. work in line with your organizations policies and procedures
PC7. work within the limits of your job role
PC8. obtain guidance from appropriate people, where necessary
PC9. ensure your work meets the agreed requirements

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. your organizations policies, procedures and priorities for your area of work and your role and responsibilities in carrying out your work
KU2. limits of your responsibilities and when to involve others
KU3. your specific work requirements and who these must be agreed with
KU4. the importance of having a tidy work area and how to do this
KU5. how to prioritize your workload according to urgency and importance and the benefits of this
KU6. your organizations policies and procedures for dealing with confidential information and the importance of complying with these
KU7. the purpose of keeping others updated with the progress of your work
KU8. who to obtain guidance from and the typical circumstances when this may be required
KU9. the purpose and value of being flexible and adapting work plans to reflect change
KU10. the importance of completing work accurately and how to do this
KU11. appropriate timescales for completing your work and the implications of not meeting these for you and the organization
KU12. resources needed for your work and how to obtain and use these

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate work with attention to detail
GS2. read instructions, guidelines, procedures, rules and service level agreements
GS3. ask for clarification and advice from line managers
GS4. communicate orally with colleagues
GS5. make decisions on suitable courses
GS6. plan and organize your work to achieve targets and deadlines
GS7. agree objectives and work requirements
GS8. deliver consistent and reliable service to customers
GS9. check your own work meets customer requirements
GS10. refer anomalies to the line manager
GS11. seek clarification on problems from others
GS12. provide relevant information to others
GS13. analyze needs, requirements and dependencies in order to meet your work requirements
GS14. apply judgments to different situations
GS15. check your work is complete and free from errors
GS16. get your work checked by peers
GS17. work effectively in a team environment
GS18. use information technology effectively, to input and/or extract data accurately
GS19. identify and refer anomalies in data
GS20. store and retrieve information
GS21. keep up to date with changes, procedures and practices in your role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	25	**75**	**-**	**-**
PC1. establish and agree your work requirements with appropriate people	-	6.25	-	-
PC2. keep your immediate work area clean and tidy	6.25	6.25	-	-
PC3. utilize your time effectively	6.25	6.25	-	-
PC4. use resources correctly and efficiently	6.25	12.5	-	-
PC5. treat confidential information correctly	-	6.25	-	-
PC6. work in line with your organizations policies and procedures	-	12.5	-	-
PC7. work within the limits of your job role	-	6.25	-	-
PC8. obtain guidance from appropriate people, where necessary	-	6.25	-	-
PC9. ensure your work meets the agreed requirements	6.25	12.5	-	-
NOS Total	**25**	**75**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9001
NOS Name	Manage your work to meet requirements
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Across all occupations
NSQF Level	4
Credits	TBD
Version	1.0
Last Reviewed Date	27/01/2022
Next Review Date	27/01/2025
NSQC Clearance Date	27/01/2022

SSC/N9002: Work effectively with colleagues

Description

This unit is about working effectively with colleagues, either in your own work group or in other work groups within your organization.

Scope

This unit/task covers the following: Colleagues:

- line manager
- members of your own work group
- people in other work groups in your organization Communicate:
- face-to-face
- by telephone
- in writing

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. communicate with colleagues clearly, concisely and accurately

PC2. work with colleagues to integrate your work effectively with theirs

PC3. pass on essential information to colleagues in line with organizational requirements

PC4. work in ways that show respect for colleagues

PC5. carry out commitments you have made to colleagues

PC6. let colleagues know in good time if you cannot carry out your commitments, explaining the reasons

PC7. identify any problems you have working with colleagues and take the initiative to solve these problems

PC8. follow the organizations policies and procedures for working with colleagues

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. your organizations policies and procedures for working with colleagues and your role and responsibilities in relation to this

KU2. the importance of effective communication and establishing good working relationships with colleagues

KU3. different methods of communication and the circumstances in which it is appropriate to use these

KU4. benefits of developing productive working relationships with colleagues

KU5. the importance of creating an environment of trust and mutual respect in an environment where you have no authority over those you are working with

KU6. where you do not meet your commitments, the implications this will have on individuals and the organization

KU7. different types of information that colleagues might need and the importance of providing this information when it is required

KU8. the importance of understanding problems from your colleagues perspective and how to provide support, where necessary, to resolve these

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate, well written work with attention to detail

GS2. communicate effectively with colleagues in writing

GS3. read instructions, guidelines, procedures, rules and service level agreements

GS4. listen effectively and orally communicate information accurately

GS5. ask for clarification and advice from line managers

GS6. make decisions on suitable courses of action

GS7. plan and organize your work to achieve targets and deadlines

GS8. check your own work meets customer requirements

GS9. deliver consistent and reliable service to customers

GS10. apply problem solving approaches in different situations

GS11. apply balanced judgments to different situations

GS12. check your work is complete and free from error

GS13. get your work checked by peers

GS14. work effectively in a team environment

GS15. work effectively with colleagues and other teams

GS16. treat other cultures with respect

GS17. identify and refer anomalies

GS18. help reach agreements with colleagues

GS19. keep up to date with changes, procedures and practices in yourrole

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	20	**80**	**-**	**-**
PC1. communicate with colleagues clearly, concisely and accurately	-	20	-	-
PC2. work with colleagues to integrate your work effectively with theirs	-	10	-	-
PC3. pass on essential information to colleagues in line with organizational requirements	10	-	-	-
PC4. work in ways that show respect for colleagues	-	20	-	-
PC5. carry out commitments you have made to colleagues	-	10	-	-
PC6. let colleagues know in good time if you cannot carry out your commitments, explaining the reasons	10	-	-	-
PC7. identify any problems you have working with colleagues and take the initiative to solve these problems	-	10	-	-
PC8. follow the organizations policies and procedures for working with colleagues	-	10	-	-
NOS Total	**20**	**80**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9002
NOS Name	Work effectively with colleagues
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Across all occupations
NSQF Level	4
Credits	TBD
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N9003: Maintain a healthy, safe and secure working environment

Description

This unit is about monitoring your working environment and making sure it meets requirements for health, safety and security

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. comply with your organizations current health, safety and security policies and procedures

PC2. report any identified breaches in health, safety, and security policies and procedures to the designated person

PC3. identify and correct any hazards that you can deal with safely, competently and within the limits of your authority

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

PC5. follow your organizations emergency procedures promptly, calmly, and efficiently

PC6. identify and recommend opportunities for improving health, safety, and security to the designated person

PC7. complete any health and safety records legibly and accurately

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. legislative requirements and organizations procedures for health, safety and security and your role and responsibilities in relation to this

KU2. what is meant by a hazard, including the different types of health and safety hazards that can be found in the workplace

KU3. how and when to report hazards

KU4. limits of your responsibility for dealing with hazards

KU5. your organizations emergency procedures for different emergency situations and the importance of following these

KU6. the importance of maintaining high standards of health, safety and security

KU7. implications that any non-compliance with health, safety and security may have on individuals and the organization

KU8. different types of breaches in health, safety and security and how and when to report these

KU9. evacuation procedures for workers and visitors

KU10. how to summon medical assistance and the emergency services, where necessary

KU11. how to use the health, safety and accident reporting procedures and the importance of these

KU12. government agencies in the areas of safety, health and security and their norms and services

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate, well written work with attention to detail
GS2. read instructions, guidelines, procedures, rules and service level agreements
GS3. listen effectively and orally communicate information accurately
GS4. make decisions on suitable courses of action
GS5. plan and organize your work to meet health, safety and security requirements
GS6. build and maintain positive and effective relationships with colleagues and customers
GS7. apply problem solving approaches in different situations
GS8. analyze data and activities
GS9. apply balanced judgments to different situations
GS10. check your work is complete and free from errors
GS11. get your work checked by peers
GS12. work effectively in a team environment
GS13. identify and refer anomalies
GS14. help reach agreements with colleagues
GS15. keep up to date with changes, procedures and practices in your role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	30	**70**	**-**	**-**
PC1. comply with your organizations current health, safety and security policies and procedures	10	10	-	-
PC2. report any identified breaches in health, safety, and security policies and procedures to the designated person	-	10	-	-
PC3. identify and correct any hazards that you can deal with safely, competently and within the limits of your authority	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	-	-
PC5. follow your organizations emergency procedures promptly, calmly, and efficiently	10	10	-	-
PC6. identify and recommend opportunities for improving health, safety, and security to the designated person	-	10	-	-
PC7. complete any health and safety records legibly and accurately	-	10	-	-
NOS Total	**30**	**70**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9003
NOS Name	Maintain a healthy, safe and secure working environment
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Across all occupations
NSQF Level	4
Credits	TBD
Version	1.0
Last Reviewed Date	27/01/2022
Next Review Date	27/01/2025
NSQC Clearance Date	27/01/2022

SSC/N9004: Provide data/information in standard formats

Description

This unit is about providing specified data/information related to your work in templates or other standard formats.

Scope

This unit/task covers the following: Appropriate people:

- line manager
- members of your own work group
- people in other work groups in your organization
- subject matter experts Data/information:
- Quantitative
- QualitativeSources:
- within your organization
- outside your organization Formats:
- paper-based
- electronic

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

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

PC2. obtain the data/information from reliable sources

PC3. check that the data/information is accurate, complete and up-to-date

PC4. obtain advice or guidance from appropriate people where there are problems with the data/information

PC5. carry out rule-based analysis of the data/information, if required

PC6. insert the data/information into the

PC7. check the accuracy of your work, involving colleagues where required

PC8. report any unresolved anomalies in the data/information to appropriate people

PC9. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. your organizations procedures and guidelines for providing data/information in standard formats and your role and responsibilities in relation to this

KU2. the knowledge management culture of your organization

KU3. your organizations policies and procedures for recording and sharing information and the importance of complying with these
KU4. the importance of validating data/information before use and how to do this
KU5. procedures for updating data in appropriate formats and with proper validation
KU6. the purpose of the CRM database
KU7. how to use the CRM database to record and extract information
KU8. the importance of having your data/information reviewed by others
KU9. the scope of any data/information requirements including the level of detail required
KU10. the importance of keeping within the scope of work and adhering to timescales
KU11. data/information you may need to provide including the sources and how to do this
KU12. templates and formats used for data/information including their purpose and how to use these
KU13. different techniques used to obtain data/information and how to apply these
KU14. how to carry out rule-based analysis on the data/information
KU15. typical anomalies that may occur in data/information
KU16. who to go to in the event of inaccurate data/information and how to report this

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate, well written work with attention to detail
GS2. read instructions, guidelines, procedures, rules and service level agreements
GS3. listen effectively and orally communicate information accurately
GS4. follow rule-based decision-making processes
GS5. make decisions on suitable courses of action
GS6. plan and organize your work to achieve targets and deadlines
GS7. check your own work meets customer requirements
GS8. meet and exceed customer expectations
GS9. apply problem solving approaches in different situations
GS10. configure data and disseminate relevant information to others
GS11. apply balanced judgments to different situations
GS12. check your work is complete and free from errors
GS13. get your work checked by peers
GS14. work effectively in a team environment
GS15. use information technology effectively, to input and/or extract data accurately
GS16. validate and update data
GS17. identify and refer anomalies in data
GS18. store and retrieve information
GS19. share information using standard formats and templates
GS20. keep up to date with changes, procedures and practices in your role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	25	**75**	**-**	**-**
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	12.5	-	-	-
PC2. obtain the data/information from reliable sources	-	12.5	-	-
PC3. check that the data/information is accurate, complete and up-to-date	6.25	6.25	-	-
PC4. obtain advice or guidance from appropriate people where there are problems with the data/information	-	6.25	-	-
PC5. carry out rule-based analysis of the data/information, if required	-	25	-	-
PC6. insert the data/information into the	-	12.5	-	-
PC7. check the accuracy of your work, involving colleagues where required	-	6.25	-	-
PC8. report any unresolved anomalies in the data/information to appropriate people	6.25	-	-	-
PC9. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time	-	6.25	-	-
NOS Total	**25**	**75**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9004
NOS Name	Provide data/information in standard formats
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Across all occupations
NSQF Level	4
Credits	TBD
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N9005: Develop your knowledge, skills and competence

Description

This unit is about taking action to ensure you have the knowledge and skills you need to perform competently in your current job role and to take on new responsibilities, where required. Competence is defined as: the application of knowledge and skills to perform to the standards required.

Scope

This unit/task covers the following: Appropriate people may be:

- line manager
- human resources specialists
- learning and development specialists
- peers Job role:
- current responsibilities as defined in your job description
- possible future responsibilities Learning and development activities:
- formal education and training programs, leading to certification
- non-formal activities (such as private study, learning from colleagues, project work), designed to meet learning and development objectives but without certification Appropriate action may be:
- undertaking further learning and development activities
- finding further opportunities to apply your knowledge and skills

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. obtain advice and guidance from appropriate people to develop your knowledge, skills and competence

PC2. identify accurately the knowledge and skills you need for your job role

PC3. identify accurately your current level of knowledge, skills and competence and any learning and development needs

PC4. agree with appropriate people a plan of learning and development activities to address your learning needs

PC5. undertake learning and development activities in line with your plan

PC6. apply your new knowledge and skills in the workplace, under supervision

PC7. obtain feedback from appropriate people on your knowledge and skills and how effectively you apply them

PC8. review your knowledge, skills and competence regularly and take appropriate action

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. your organizations procedures and guidelines for developing your knowledge, skills and competence and your role and responsibilities in relation to this

KU2. the importance of developing your knowledge, skills and competence to you and your organization

KU3. different methods used by your organization to review skills and knowledge including: training need analysis skills need analysis performance appraisals

KU4. how to review your knowledge and skills against your job role using different methods and analyses

KU5. different types of learning and development activities available for your job role and how to access these

KU6. how to produce a plan to address your learning and development needs, who to agree it with and the importance of undertaking the planned activities

KU7. different types of support available to help you plan and undertake learning and development activities and how to access these

KU8. why it is important to maintain records of your learning and development

KU9. methods of obtaining and accepting feedback from appropriate people on your knowledge skills and competence

KU10. how to use feedback to develop in your job role

KU11. the knowledge and skills required in your job role

KU12. your current learning and development needs in relation to your job role

KU13. different types of learning styles and methods including those that help you learn best

KU14. the importance of taking responsibility for your own learning and development

KU15. to the importance of learning and practicing new concepts, theory and how to apply these in the work environment or on samples

KU16. how to explore sample problems and apply solutions

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. communicate with colleagues in writing

GS2. read instructions, guidelines, procedures

GS3. ask for clarification and advice from line managers

GS4. make decisions on suitable courses of action

GS5. plan and organize your work to achieve targets and deadlines

GS6. check your own work meets customer requirements

GS7. refer anomalies to the line manager

GS8. analyze data and activities

GS9. apply balanced judgments to different situations

GS10. check your work is complete and free from errors

GS11. get your work checked by peers

GS12. work effectively in a team environment

GS13. use information technology effectively

GS14. agree objectives and work requirements

GS15. keep up to date with changes, procedures and practices in your role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	20	**80**	**-**	**-**
PC1. obtain advice and guidance from appropriate people to develop your knowledge, skills and competence	-	10	-	-
PC2. identify accurately the knowledge and skills you need for your job role	-	10	-	-
PC3. identify accurately your current level of knowledge, skills and competence and any learning and development needs	10	10	-	-
PC4. agree with appropriate people a plan of learning and development activities to address your learning needs	-	10	-	-
PC5. undertake learning and development activities in line with your plan	10	10	-	-
PC6. apply your new knowledge and skills in the workplace, under supervision	-	10	-	-
PC7. obtain feedback from appropriate people on your knowledge and skills and how effectively you apply them	-	10	-	-
PC8. review your knowledge, skills and competence regularly and take appropriate action	-	10	-	-
NOS Total	**20**	**80**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9005
NOS Name	Develop your knowledge, skills and competence
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Across all occupations
NSQF Level	4
Credits	TBD
Version	1.0
Last Reviewed Date	16/12/2019
Next Review Date	16/12/2024
NSQC Clearance Date	NA

Assessment Guidelines and Assessment Weightage

Assessment Guidelines

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

2. The assessment for the theory part will be based on knowledge bank of questions created by the SSC.

3. Individual assessment agencies will create unique question papers for theory part for each candidate at each examination/training center (as per assessment criteria below).

4. Individual assessment agencies will create unique evaluations for skill practical for every student at each examination/ training center based on these criteria.

5. In case of successfully passing only certain number of NOSs, the trainee is eligible to take subsequent assessment on the balance NOS's to pass the Qualification Pack.

6. In case of unsuccessful completion, the trainee may seek reassessment on the Qualification Pack

Minimum Aggregate Passing % at QP Level : 70

(**Please note**: Every Trainee should score a minimum aggregate passing percentage as specified above, to successfully clear the Qualification Pack assessment.)

Assessment Weightage

Compulsory NOS

National Occupational Standards	Theory Marks	Practical Marks	Project Marks	Viva Marks	Total Marks	Weightage
SSC/N0918.Maintain compliance to information security policies, regulations and standards andaddress risk issues	32	68	-	-	100	10
SSC/N0922.Provide network security recommendations as per requirements	32	68	-	-	100	10
SSC/N0923.Carry out configuration review and provide recommendations for secure configuration of networks and security devices	32	68	-	-	100	10
SSC/N0925.Test, run exploits to identify vulnerabilities in networks	30	70	-	-	100	10
SSC/N0927.Drive interrelated cyber security actions	35	65	-	-	100	10
SSC/N0928.Manage a project team	32	68	-	-	100	10
SSC/N9001.Manage your work to meet requirements	25	75	-	-	100	8
SSC/N9002.Work effectively with colleagues	20	80	-	-	100	8
SSC/N9003.Maintain a healthy, safe and secure working environment	30	70	-	-	100	8

National Occupational Standards	Theory Marks	Practical Marks	Project Marks	Viva Marks	Total Marks	Weightage
SSC/N9004.Provide data/information in standard formats	25	75	-	-	100	8
SSC/N9005.Develop your knowledge, skills and competence	20	80	-	-	100	8
Total	**313**	**787**	**-**	**-**	**1100**	**100**

Acronyms

NOS	National Occupational Standard(s)
NSQF	National Skills Qualifications Framework
QP	Qualifications Pack
TVET	Technical and Vocational Education and Training
IT-ITeS	Information Technology - Information Technology enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	Legal Process Outsourcing
IPO	Information Process Outsourcing
BCA	Bachelor of Computer Applications
B.Sc	. Bachelor of Science
B.Sc	Bachelor of Science

Glossary

Sector	Sector is a conglomeration of different business operations having similar business and interests. It may also be defined as a distinct subset of the economy whose components share similar characteristics and interests.
Sub-sector	Sub-sector is derived from a further breakdown based on the characteristics and interests of its components.
Occupation	Occupation is a set of job roles, which perform similar/ related set of functions in an industry.
Job role	Job role defines a unique set of functions that together form a unique employment opportunity in an organisation.
Occupational Standards (OS)	OS specify the standards of performance an individual must achieve when carrying out a function in the workplace, together with the Knowledge and Understanding (KU) they need to meet that standard consistently. Occupational Standards are applicable both in the Indian and global contexts.
Performance Criteria (PC)	Performance Criteria (PC) are statements that together specify the standard of performance required when carrying out a task.
National Occupational Standards (NOS)	NOS are occupational standards which apply uniquely in the Indian context.
Qualifications Pack (QP)	QP comprises the set of OS, together with the educational, training and other criteria required to perform a job role. A QP is assigned a unique qualifications pack code.
Unit Code	Unit code is a unique identifier for an Occupational Standard, which is denoted by an 'N'
Unit Title	Unit title gives a clear overall statement about what the incumbent should be able to do.
Description	Description gives a short summary of the unit content. This would be helpful to anyone searching on a database to verify that this is the appropriate OS they are looking for.
Scope	Scope is a set of statements specifying the range of variables that an individual may have to deal with in carrying out the function which have a critical impact on quality of performance required.

Knowledge and Understanding (KU)	Knowledge and Understanding (KU) are statements which together specify the technical, generic, professional and organisational specific knowledge that an individual needs in order to perform to the required standard.
Organisational Context	Organisational context includes the way the organisation is structured and how it operates, including the extent of operative knowledge managers have of their relevant areas of responsibility.
Technical Knowledge	Technical knowledge is the specific knowledge needed to accomplish specific designated responsibilities.
Core Skills/ Generic Skills (GS)	Core skills or Generic Skills (GS) are a group of skills that are the key to learning and working in today's world. These skills are typically needed in any work environment in today's world. These skills are typically needed in any work environment. In the context of the OS, these include communication related skills that are applicable to most job roles.
Electives	Electives are NOS/set of NOS that are identified by the sector as contributive to specialization in a job role. There may be multiple electives within a QP for each specialized job role. Trainees must select at least one elective for the successful completion of a QP with Electives.
Options	Options are NOS/set of NOS that are identified by the sector as additional skills. There may be multiple options within a QP. It is not mandatory to select any of the options to complete a QP with Options.
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk.

Consultant Network Security

QP Code: SSC/Q0917

Version: 2.0

NSQF Level: 8

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

Contents

SSC/Q0917: Consultant Network Security

Brief Job Description

This job role is responsible for understanding network security needs from stakeholders and vulnerability analysis/penetration testing reports and researching and providing recommendations for solutions from existing network security solutions available. The consultant is also responsible for reviewing secure configuration and providing recommendations for minimum baseline security standards for all network security devices as well as for Network Security Policy and Standard operating procedures (SOPs).

Personal Attributes

This job may require the individual to work independently and take decisions for his/her own area of work. The individual should have a high level of analytical thinking ability, problem solving ability, passion for information security and attention for detail, should be ethical, compliance and result oriented, should also be able to demonstrate interpersonal and managerial skills.

Applicable National Occupational Standards (NOS)

Compulsory NOS:

1. SSC/N0918: Maintain compliance to information security policies, regulations and standards andaddress risk issues
2. SSC/N0922: Provide network security recommendations as per requirements
3. SSC/N0923: Carry out configuration review and provide recommendations for secure configuration of networks and security devices
4. SSC/N0925: Test, run exploits to identify vulnerabilities in networks
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 colleagues
9. SSC/N9004: Provide data/information in standard formats
10. SSC/N9014: Maintain an inclusive, environmentally sustainable workplace

Qualification Pack (QP) Parameters

Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information and Cyber Security
Country	India
NSQF Level	8
Aligned to NCO/ISCO/ISIC Code	NCO-2015/NIL
Minimum Educational Qualification & Experience	B.E./B.Tech (Security/ Computer Science/Electronics and Engineering/Information Technology) with 2-3 Years of experience Information technology
Minimum Level of Education for Training in School	12th Class
Pre-Requisite License or Training	NA
Minimum Job Entry Age	21 Years
Last Reviewed On	16/07/2020
Next Review Date	16/07/2025
NSQC Approval Date	
Version	2.0

SSC/N0918: Maintain compliance to information security policies, regulations and standards andaddress risk issues

Description

This unit is about maintaining compliance to information security policies, regulations and standards and address risk issues in organizations.

Scope

This unit/task covers the following:Operating procedures include:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityCompliance audit and risk assessment:
- executive briefings
- risk assessment reports
- dashboardsProfessional and technical knowledge:
- by attending educational workshops
- reviewing professional publications
- establishing personal networks
- benchmarking state-of-the-art practices
- participating in professional societiesBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code like o viruso Trojano logic bombo wormo spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etc.

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. communicate the subsequent compliance audit and risk assessment results to specified organizational personnel

PC2. share compliance issues identified during the audit with appropriate organizational personnel as per process laid out

PC3. plan and coordinate the operational activities of a given company or organization to guarantee compliance with governmental regulations, ordinances and standards

PC4. ensure that all policies and procedures are implemented and well documented

PC5. perform occasional internal reviews, and identify compliance problems that call for formal attention

PC6. file compliance reports with regulatory bodies

PC7. take necessary actions for closure of the risk and nonconformance issues during the lifecycle

PC8. present compliance issues identified to the management for prioritizing, support risk mitigation plan

PC9. co-ordinate for ongoing monitoring of the risk factors to organizational operations and assets, individuals, other organizations

PC10. undertake corrective actions or implementation of controls or procedural steps for satisfying needs of compliances

PC11. implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service

PC12. maintain quality service by establishing and enforcing organization standards

PC13. maintain legal and regulatory compliance by researching and communicating requirements, and obtain approvals

PC14. maintain regular communication and contact with organizational head and other departments to share information and to ensure that compliance related activities are coordinated

PC15. document steps undertaken during the process & outcomes of the steps taken

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

PC17. complete research assignments and deliver comprehensive but concise reports in a timely manner

PC18. provide timely feedback on contracts and agreements to be issued or entered into by the organization

PC19. maintain professional and technical knowledge by formal and informal means

PC20. ensure that customer needs are met within SLA and meet other time and quality commitment KPIs

PC21. maintain a collaborative relationship with various stakeholders like management, other function heads and point of contacts, etc

PC22. provide guidance and suggestions as appropriate

PC23. complete own assigned tasks and activities to defined standards and timelines

PC24. correctly follow and apply the policies and standards relating to information security identity and access management activities

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. Organizational hierarchy and management structure

KU6. Legal and regulatory guidelines applicable to the business or domain that the organization is engaged in

KU7. how to engage with both internal and external specialists for support in order to resolve incidents and service requests
KU8. service request procedures, tools, and techniques
KU9. the operating procedures that are applicable to the system(s) being used
KU10. typical response times and service times related to own work area
KU11. computer network defense (CND) policies, procedures, and regulations
KU12. Basic cyber security concepts
KU13. explain how hardware and software vulnerabilities can be identified and resolved
KU14. what is meant by risk management, risk mitigation and risk control and what these entail
KU15. what are the aims and objectives of risk management
KU16. activities that are involved in the management of risk
KU17. the procedures, tools and techniques that can be used to conduct and document risk assessment activities
KU18. known vulnerabilities from alerts, advisories, errata, and bulletins
KU19. business objectives of the organization
KU20. the steps involved in information security risk management
KU21. compliance policies of the organization concerned
KU22. organizational procedures for information security audits
KU23. Risk Management Framework (RMF) requirements
KU24. information technology (IT) supply chain security/risk management policies, requirements, and procedures
KU25. various types of controls and safeguards for cyber security
KU26. computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities
KU27. systems diagnostic tools and fault identification techniques
KU28. new and emerging information technology (IT) and information security technologies
KU29. structured analysis principles and methods
KU30. names and uses of systems diagnostic tools and fault identification techniques
KU31. organizations enterprise information technology (IT) goals and objectives
KU32. relevant laws, policies, procedures, or standards as they relate to work that may impact critical infrastructure
KU33. Information Security concepts, policies, and procedures

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. document call logs, reports, task lists, and schedules with co-workers
GS2. prepare status and progress reports
GS3. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes

GS4. read about new products and services with reference to the organization and also from external forums such as websites and blogs

GS5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets

GS6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal

GS7. read policy manual, standard operating procedures and service level agreements relevant to work area

GS8. read emails received from own team, across team and external vendors and clients

GS9. discuss task lists, schedules, and work-loads with co-workers

GS10. give clear instructions to specialists/vendors/users/clients as required

GS11. keep stakeholders informed about progress

GS12. avoid using jargon, slang or acronyms when communicating with a customer,unless it is required

GS13. receive and make phone calls, including call forward, call hold, and call mute

GS14. follow rule-based decision-making processes

GS15. make decisions on suitable courses of action

GS16. plan and organize your work to achieve targets and deadlines

GS17. carry out rule-based transactions in line with customer-specific guidelines

GS18. procedures, rules and service level agreements

GS19. check your own and/or your peers work meets customer requirements

GS20. apply problem-solving approaches in different situations

GS21. seek clarification on problems from others

GS22. analyze data and activities

GS23. configure data and disseminate relevant information to others

GS24. pass on relevant information to others

GS25. provide opinions on work in a detailed and constructive way

GS26. apply balanced judgments to different situations

GS27. apply good attention to details

GS28. check your work is complete and free from errors

GS29. work effectively in a team environment

GS30. contribute to the quality of team working

GS31. work independently and collaboratively

GS32. determine how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes

GS33. identify measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system

GS34. evaluate the trustworthiness of the supplier and/or product

GS35. work on various operating systems

GS36. work with word processors, spreadsheets and presentations

GS37. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. communicate the subsequent compliance audit and risk assessment results to specified organizational personnel	1	3	-	-
PC2. share compliance issues identified during the audit with appropriate organizational personnel as per process laid out	1	3	-	-
PC3. plan and coordinate the operational activities of a given company or organization to guarantee compliance with governmental regulations, ordinances and standards	2	3	-	-
PC4. ensure that all policies and procedures are implemented and well documented	1	3	-	-
PC5. perform occasional internal reviews, and identify compliance problems that call for formal attention	2	3	-	-
PC6. file compliance reports with regulatory bodies	1	2	-	-
PC7. take necessary actions for closure of the risk and nonconformance issues during the lifecycle	2	3	-	-
PC8. present compliance issues identified to the management for prioritizing, support risk mitigation plan	2	3	-	-
PC9. co-ordinate for ongoing monitoring of the risk factors to organizational operations and assets, individuals, other organizations	1	4	-	-
PC10. undertake corrective actions or implementation of controls or procedural steps for satisfying needs of compliances	2	3	-	-
PC11. implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service	2	3	-	-
PC12. maintain quality service by establishing and enforcing organization standards	1	3	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC13. maintain legal and regulatory compliance by researching and communicating requirements, and obtain approvals	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	1	3	-	-
PC15. document steps undertaken during the process & outcomes of the steps taken	1	2	-	-
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	1	2	-	-
PC17. complete research assignments and deliver comprehensive but concise reports in a timely manner	2	3	-	-
PC18. provide timely feedback on contracts and agreements to be issued or entered into by the organization	1	3	-	-
PC19. maintain professional and technical knowledge by formal and informal means	1	3	-	-
PC20. ensure that customer needs are met within SLA and meet other time and quality commitment KPIs	1	2	-	-
PC21. maintain a collaborative relationship with various stakeholders like management, other function heads and point of contacts, etc	1	3	-	-
PC22. provide guidance and suggestions as appropriate	2	2	-	-
PC23. complete own assigned tasks and activities to defined standards and timelines	1	3	-	-
PC24. correctly follow and apply the policies and standards relating to information security identity and access management activities	1	3	-	-
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0918
NOS Name	Maintain compliance to information security policies, regulations and standards andaddress risk issues
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	7
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0922: Provide network security recommendations as per requirements

Description

This unit is about identifying needs, researching and recommending network security solutions as per requirements.

Scope

This unit/task covers the following:Operating procedures includes:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentiality Network security measures are:
- firewall, to keep unauthorized users off the network
- virtual private network (VPN), to give employees, customers, and partners secure access to the network
- intrusion prevention, to detect and stop threats before they harm the network
- content security, to protect the network from viruses, spam, spyware, and other attacks
- secure wireless network, to provide safe network access to visitors and employees on the go
- identity management, to give the business owner control over who and what can access the network
- compliance validation, to make sure that any device accessing the network
- meets the security requirement deep packet inspectionBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code likeo viruso Trojano logic bombo wormo spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etcRelevant networking concepts, devices and terminology such as:
- Concepts: OSI Model/topology; Network Protocols, bandwidth management, etc.
- Devices and databases: Switches, routers, Intrusion detection and prevention System (IDPS), etc.
- Terminology: SSL, VPN, 2FA, Encryption, IPSEC, TLS, IP subnetting, network routing, RADIUS, TACACS+etc.Tools and technologies used in network security include but are not limited to:
- IP Scanners
- Sniffers
- Bandwidth Monitoring
- Network Monitoring tool
- Packet analyser
- Computer network defence (CND)Security principles and methods are:
- firewalls
- demilitarized zones
- encryption

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. consult with customers to evaluate functional requirements for network security

PC2. define project scope and objectives based on customer requirements

PC3. confirm availability of complete and accurate details of the security objectives

PC4. Evaluate the existing network protocols and topology of users

PC5. review the usage of existing network security measures, and assess risks w.r.t security objectives

PC6. consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements

PC7. conduct technical risk analysis, threat identification of the existing network security measures

PC8. identify level of risk acceptable for business requirements by discussing with business and technical leads

PC9. critically interpret information and data, from both within the customer/client organisation and other sources, in order to identify network security requirements

PC10. research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks

PC11. identify and record details of constraints that may have an impact on the business and security options

PC12. explore potential vulnerabilities that could be technical, operational or management related

PC13. categorize vulnerabilities and identify extent of vulnerability including level of weakness and sensitivity of the information

PC14. identify the root cause of vulnerabilities

PC15. research options of network security solutions that match the and security requirements captured

PC16. gather sufficient accurate information on which to determine potential costs, benefits and effectiveness of potential security solutions

PC17. identify and determine the cost, potential benefits, and effectiveness of recommended security solutions, based on valid assumptions, considerations and information, including possible constraints

PC18. prepare recommendations that have the potential to meet the security objectives of the organisation

PC19. provide details of costs, benefits, effectiveness, limitations and constraints of recommendations

PC20. provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales

PC21. provide the organisation with considered advice on the implications of accepting, modifying or rejecting security recommendations

PC22. co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs

PC23. take account of the organisations values, culture and nature of business

PC24. maintain the security and confidentiality of information relating to your organisation and recommendations

PC25. obtain necessary approvals from the responsible persons as per organisational policy
PC26. evaluate ways & means of closing weaknesses in the network
PC27. maintain logs for all the activities performed

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company
KU2. organizations knowledge base and how to access and update this
KU3. limits of your role and responsibilities and who to seek guidance from
KU4. he organizational systems, procedures and tasks/checklists within the domain and how to use these
KU5. the operating procedures that are applicable to the system(s) being used
KU6. typical response times and service times related to own work area
KU7. standard tools and templates available and how to use these
KU8. basic cyber security concepts
KU9. how hardware and software vulnerabilities can be identified and resolved
KU10. relevant networking concepts, devices and terminology
KU11. network security principles and processes
KU12. network security tools, technologies and applications
KU13. vulnerability analysis and penetration testing report templates
KU14. various sources for researching for existing network security solution
KU15. categorization and root cause analysis process of vulnerabilities
KU16. types of addresses used on networks and why they are used
KU17. basics of enterprise information technology (IT) architecture Information Technology Architecture
KU18. extension points of the products (for customization and integration with other applications)
KU19. secure integration approach with different third party systems
KU20. statutory knowledge (IT Act, TRAI Guidelines, and other national and international Guidelines)
KU21. standards and industry best practices for network security
KU22. new technological developments in Network security
KU23. principles and methods for integrating technology components
KU24. traffic analysis using flow and pcaps
KU25. server administration and systems engineering theories, concepts, and methods Systems Life Cycle
KU26. Segregation of Duties (SoD) configuration
KU27. migration of systems and users
KU28. the basic functionalities of the applications, hardware and/or access rights that are used by the customers
KU29. host/network access controls (e.g., access control list)
KU30. Advanced knowledge of cloud security

KU31. intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate well written work with attention to detail
GS2. document call logs, reports, task lists, and schedules with co-workers
GS3. prepare status and progress reports
GS4. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes
GS5. write standard operating procedures (SOPs) and reports relevant to work area
GS6. read about new products and services with reference to the organization and also from external forums such as websites and blogs
GS7. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets
GS8. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal
GS9. read policy manual, standard operating procedures and service level agreements relevant to work area
GS10. read emails received from own team, across team and external vendors and clients
GS11. discuss task lists, schedules, and work-loads with co-workers
GS12. solicit and record information by asking pertinent questions from various stakeholders
GS13. give clear instructions to specialists/vendors/users/clients as required
GS14. make presentations to stakeholders
GS15. keep stakeholders informed about progress through MIS reports
GS16. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required
GS17. receive and make phone calls, including call forward, call hold, and call mute
GS18. follow rule-based decision-making processes
GS19. make a decision on a suitable course of action
GS20. plan and organize your work to achieve targets and deadlines
GS21. Identify internal or external customer requirement and priorities clearly with respect to work at hand
GS22. carry out rule-based transactions in line with customer-specific guidelines, procedures, rules and service level agreements
GS23. check that your own and/or your peers work meets customer requirements
GS24. apply problem-solving approaches in different situations
GS25. seek clarification on problems from others
GS26. analyze data and activities
GS27. configure data and disseminate relevant information to others
GS28. pass on relevant information to others

GS29. provide opinions on work in a detailed and constructive way

GS30. apply balanced judgments to different situations

GS31. check your work is complete and free from errors

GS32. work effectively in a team environment

GS33. work independently and collaboratively

GS34. configure, diagnose and troubleshoot computer networks using in-depth understanding of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], HTTPS, SSH, FTP, Dynamic Host Configuration Protocol [DHCP]) and directory services (e.g., Domain Name System [DNS])

GS35. administer, use and monitor of an intrusion detection system

GS36. Install and configure firewalls, routers, Intrusion detection and prevention System(IDPS)

GS37. read and write coded scripts and modify and debug programs

GS38. collect data from a variety of computer network defense resources

GS39. work on various operating system

GS40. work with word processers, spreadsheets and presentations

GS41. perform basic penetration testing and ethical hacking

GS42. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. consult with customers to evaluate functional requirements for network security	1	3	-	-
PC2. define project scope and objectives based on customer requirements	1	3	-	-
PC3. confirm availability of complete and accurate details of the security objectives	1	2	-	-
PC4. Evaluate the existing network protocols and topology of users	2	2	-	-
PC5. review the usage of existing network security measures, and assess risks w.r.t security objectives	2	2	-	-
PC6. consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements	1	3	-	-
PC7. conduct technical risk analysis, threat identification of the existing network security measures	2	3	-	-
PC8. identify level of risk acceptable for business requirements by discussing with business and technical leads	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	1	3	-	-
PC10. research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks	1	3	-	-
PC11. identify and record details of constraints that may have an impact on the business and security options	1	2	-	-
PC12. explore potential vulnerabilities that could be technical, operational or management related	2	3	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC13. categorize vulnerabilities and identify extent of vulnerability including level of weakness and sensitivity of the information	2	2	-	-
PC14. identify the root cause of vulnerabilities	1	3	-	-
PC15. research options of network security solutions that match the and security requirements captured	1	4	-	-
PC16. gather sufficient accurate information on which to determine potential costs, benefits and effectiveness of potential security solutions	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	1	2	-	-
PC18. prepare recommendations that have the potential to meet the security objectives of the organisation	1	3	-	-
PC19. provide details of costs, benefits, effectiveness, limitations and constraints of recommendations	1	2	-	-
PC20. provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales	1	2	-	-
PC21. provide the organisation with considered advice on the implications of accepting, modifying or rejecting security recommendations	1	2	-	-
PC22. co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs	1	3	-	-
PC23. take account of the organisations values, culture and nature of business	1	2	-	-
PC24. maintain the security and confidentiality of information relating to your organisation and recommendations	1	2	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC25. obtain necessary approvals from the responsible persons as per organisational policy	1	2	-	-
PC26. evaluate ways & means of closing weaknesses in the network	1	3	-	-
PC27. maintain logs for all the activities performed	1	2	-	-
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0922
NOS Name	Provide network security recommendations as per requirements
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0923: Carry out configuration review and provide recommendations for secure configuration of networks and security devices

Description

This unit is about carrying out configuration review and providing recommendations for secure configuration of networks and security devices.

Scope

This unit/task covers the following:Various means of protecting configuration files include but are not limited to:

- encode and Encrypt and/or a salted hash with iteration to protect confidentiality of passwords in configuration files
- change passwords/keys immediately if the network device configuration file is transmitted in the clear (or is otherwise exposed) while containing non-encrypted passwords/keys Operating procedures includes:
- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code likeo viruso Trojano logic bombo wormo spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etc.Relevant networking concepts, devices and terminology such as:
- Concepts: OSI Model/topology; Network Protocols, bandwidth management, etc.
- Devices and databases: Switches, routers, Intrusion detection and prevention System (IDPS), etc.
- Terminology: SSL, VPN, 2FA, Encryption, IPSEC, TLS, IP subnetting, network routing, RADIUS, TACACS+etc.Security principles and methods are:
- firewalls
- demilitarized zones
- encryption

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. conduct an inventory to identify the network configuration items that need to be secured

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

PC3. identify and record the configurations of network configuration items that impact the cyber security posture of the organization

PC4. review initial configuration of network configuration items considering security vulnerabilities and threats identified

PC5. provide recommendations for secure configuration measures for networks considering business requirements

PC6. establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements

PC7. provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of the organization and business requirements

PC8. provide recommendation of appropriate solution for secure configuration management (SCM solution) as per requirements of the organisation

PC9. test secure configurations prior to implementation in the production environment

PC10. diagnose issues and respond to queries from the implementation team with respect to various secure configuration processes and specifications

PC11. suggest remediation actions to resolve issues caused due to erroneous network device configurations

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. the operating procedures that are applicable to the system(s) being used

KU6. typical response times and service times related to own work area

KU7. standard tools and templates available and how to use these

KU8. basic cyber security concepts

KU9. how hardware and software vulnerabilities can be identified and resolved

KU10. relevant networking concepts, devices and terminology

KU11. how to install, integrate, and optimize system components

KU12. information technology (IT) security principles and methods

KU13. network access, identity and access management

KU14. network design processes, to include understanding of security objectives, operational objectives, and tradeoffs

KU15. network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools

KU16. network traffic analysis methods

KU17. importance of secure configuration management of network devices

KU18. secure configuration management activities

KU19. secure configuration measures and process for network devices

KU20. patch Management and malware protection
KU21. available secure configuration management (SCM) solutions
KU22. system development life cycle (SDLC)
KU23. baseline configuration
KU24. process for testing the network to ascertain that it has not been breached
KU25. traffic filtering technologies and the needs they fulfill
KU26. various means of protecting configuration files
KU27. what could be sensitive data and transaction flows in an organization
KU28. process for scanning an organizations Internet address ranges
KU29. windows command line (e.g., ipconfig, netstat, dir, nbtstat)
KU30. unix command line (e.g., mkdir, mv, ls, passwd, grep)
KU31. common attack vectors on the network layer

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate well written work with attention to detail
GS2. document call logs, reports, task lists, and schedules with co-workers
GS3. Prepare status and progress reports
GS4. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes
GS5. read about new products and services with reference to the organization and also from external forums such as websites and blogs
GS6. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets
GS7. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal
GS8. read policy manual, standard operating procedures and service level agreements relevant to work area
GS9. read emails received from own team, across team and external vendors and clients
GS10. discuss task lists, schedules, and work-loads with co-workers
GS11. give clear instructions to specialists/vendors/users/clients as required
GS12. keep stakeholders informed about progress
GS13. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required
GS14. receive and make phone calls, including call forward, call hold, and call mute
GS15. follow rule-based decision-making processes
GS16. make a decision on a suitable course of action
GS17. plan and organize your work to achieve targets and deadlines
GS18. Identify internal or external customer requirement and priorities clearly with respect to work at hand

GS19. carry out rule-based transactions in line with customer-specific guidelines, procedures, rules and service level agreements

GS20. check that your own and/or your peers work meets customer requirements

GS21. apply problem-solving approaches in different situations

GS22. seek clarification on problems from others

GS23. analyze data and activities

GS24. configure data and disseminate relevant information to others

GS25. pass on relevant information to others

GS26. provide opinions on work in a detailed and constructive way

GS27. apply balanced judgments to different situations

GS28. check your work is complete and free from errors

GS29. work effectively in a team environment

GS30. work effectively in a team environment

GS31. configure, diagnose and troubleshoot computer networks using in-depth understanding of TCP/IP protocols

GS32. update firewall IP address and subnet masks

GS33. change default username and passwords of the firewall devices

GS34. administer, use and monitor of an intrusion detection system

GS35. configure firewalls and routers

GS36. update firewall IP address and subnet masks

GS37. change default username and passwords of the firewall devices

GS38. work on various operating system

GS39. work with word processers, spreadsheets and presentations

GS40. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. conduct an inventory to identify the network configuration items that need to be secured	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	3	6	-	-
PC3. identify and record the configurations of network configuration items that impact the cyber security posture of the organization	3	5	-	-
PC4. review initial configuration of network configuration items considering security vulnerabilities and threats identified	3	5	-	-
PC5. provide recommendations for secure configuration measures for networks considering business requirements	3	6	-	-
PC6. establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements	3	6	-	-
PC7. provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of the organization and business requirements	3	6	-	-
PC8. provide recommendation of appropriate solution for secure configuration management (SCM solution) as per requirements of the organisation	3	6	-	-
PC9. test secure configurations prior to implementation in the production environment	4	7	-	-
PC10. diagnose issues and respond to queries from the implementation team with respect to various secure configuration processes and specifications	3	7	-	-
PC11. suggest remediation actions to resolve issues caused due to erroneous network device configurations	2	8	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0923
NOS Name	Carry out configuration review and provide recommendations for secure configuration of networks and security devices
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0925: Test, run exploits to identify vulnerabilities in networks

Description

This unit is about performing network vulnerability assessment.

Scope

This unit/task covers the following:Operating procedures includes:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityPreliminary Information:
- scope and schedule of work
- type of assessment
- business priorities
- type of network and network components
- constraints
- already identified risks and vulnerabilities
- possible areas of weakness Information gathering tools:
- IP Scanners
- Sniffers
- Bandwidth Monitoring
- Network Monitoring tool
- packet analyser
- computer network defence (CND)sInformation gathering methods:
- conduct Search Engine Discovery and Reconnaissance for Information Leakage
- Create IP schema for all network security devices, update quarterly Active Reconnaissance:
- touching the target(network) directly Public repositories are:
- whois databases
- domain registrars
- usenet groups
- mailing lists Pivoting techniques:
- Pivoting is a process in which a penetration tester uses the compromised (target) system to attack other systems in the target network. Basic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for information systems;
- common types of malicious code likeo virus o Trojan o logic bomb o worm o spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability and motive, etc.Relevant networking concepts, devices and terminology such as:
- Concepts: OSI Model/topology; Network Protocols, bandwidth management, host network access controls, directory services, etc.

- Devices: Hubs, switches, routers, bridges, servers, transmission media, Intrusion detection and prevention System(IDPS), etc.
- Databases: Oracle, SQL, MySQL
- Terminology: SSL, VPN, 2FA, Encryption, IPSEC, TLS, IP subnetting, network routing, RADIUS, TACACS+, etc. Encryption algorithms are:
- Internet Protocol Security [IPSEC]
- Advanced Encryption Standard [AES]
- Generic Routing Encapsulation [GRE]
- Internet Key Exchange [IKE]
- Message Digest Algorithm [MD5]
- Secure Hash Algorithm [SHA]
- Triple Data Encryption Standard [3DES] Security principles and methods are:
- firewalls
- demilitarized zones
- encryption Traffic flows are:
- Transmission Control Protocol and Internet Protocol [TCP/IP]
- Open System Interconnection model [OSI]
- Information Technology Infrastructure Library
- v3 [ITIL]) Network protocols are:
- Transmission Control Protocol and Internet Protocol [TCP/IP]
- Dynamic Host Configuration Protocol [DHCP]) Directory Services are:
- Domain Name System [DNS] Windows command line
- ipconfig
- netstat
- dir
- nbtstatUnix command line
- mkdir
- mv
- ls
- passwd
- grep

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. Consult with customers to evaluate functional requirements for network security.

PC2. Define project scope and objectives based on customer requirements.

PC3. Confirm the availability of complete and accurate details of the security objectives.

PC4. Review the usage of existing network security measures, and assess risks w.r.t security objectives.

PC5. create documents using standard templates and agreed language standards

PC6. Consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements.

PC7. Conduct technical risk analysis, threat identification of the existing network security measures

PC8. Identify the level of risk acceptable for business requirements by discussing with business and technical leads

PC9. Critically interpret information and data, from both within the customer/client organization and other sources, in order to identify network security requirements.

PC10. Research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks

PC11. Identify and record details of constraints that may have an impact on the business and security options.

PC12. Explore potential vulnerabilities that could be technical, operational or management related .

PC13. Categorize vulnerabilities and identify the extent of vulnerability including the level of weakness and sensitivity of the information .

PC14. Identify the root cause of vulnerabilities.

PC15. Research options of network security solutions that match the productivity and security requirements captured .

PC16. Gather sufficient accurate information on which to determine potential costs, benefits , and effectiveness of potential security solutions .

PC17. Identify and determine the cost, potential benefits, and effectiveness of recommended security solutions, based on valid assumptions, considerations , and information, including possible constraints .

PC18. Prepare recommendations that have the potential to meet the security objectives of the organization.

PC19. Provide details of costs, benefits, effectiveness, limitations , and constraints of recommendations

PC20. Provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales .

PC21. Provide the organization with considered advice on the implications of accepting, modifying or rejecting security recommendations .

PC22. Co ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs .

PC23. Take account of the organizations values, culture , and nature of the business .

PC24. Maintain the security and confidentiality of information relating to your organization and recommendations.

PC25. Obtain necessary approvals from the responsible persons as per organizational policy.

PC26. Evaluate ways & means of closing weaknesses in the network.

PC27. Maintain logs for all the activities performed

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. organizations knowledge base and how to access and update this

KU2. limits of your role and responsibilities and who to seek guidance from

KU3. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU4. the operating procedures that are applicable to the system(s) being used

KU5. typical response times and service times related to own work area

KU6. standard tools and templates available and how to use these

KU7. basic cyber security concepts
KU8. explain how hardware and software vulnerabilities can be identified and resolved
KU9. relevant networking concepts, devices and terminology
KU10. known vulnerabilities from alerts, advisories, errata, and bulletins
KU11. encryption algorithms
KU12. information technology (IT) security principles and methods
KU13. network access, identity, and access management
KU14. network design processes, to include understanding of security objectives, operational objectives, and tradeoffs
KU15. operating systems
KU16. how traffic flows across the network
KU17. parallel and distributed computing concepts
KU18. systems testing and evaluation methods
KU19. vulnerability assessment tools, including open source tools, and their capabilities
KU20. host/network access controls (e.g., access control list)
KU21. intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies
KU22. network traffic analysis methods
KU23. what constitutes a network attack and the relationship to both threats and vulnerabilities
KU24. Various types of network security devices, their roles and hardening requirements
KU25. standard System Development Life Cycle (SDLC) practices and process
KU26. patch management and its importance
KU27. importance of regular operation and maintenance on network security devices and what does it include
KU28. windows command line
KU29. unix command line
KU30. the common attack vectors on the network layer
KU31. internet ports, protocols and services and their usefulness
KU32. security solutions like Firewall, Intrusion detection and prevention System (IDPS), web security gateways, email security, content management, etc.
KU33. new technological developments in network security
KU34. basics of mobile network security and cloud network security
KU35. key features of mobile and cloud network testing tools

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate well written work with attention to detail
GS2. document call logs, reports, task lists, and schedules with co-workers
GS3. prepare status and progress reports
GS4. log calls and raise tickets in the SIEM tool, providing proper indicators and descriptions as required

GS5. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes

GS6. read about new products and services with reference to the organization and also from external forums such as websites and blogs

GS7. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets

GS8. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal

GS9. read policy manual, standard operating procedures and service level agreements relevant to work area

GS10. read emails received from own team, across team and external vendors and clients

GS11. discuss task lists, schedules, and work-loads with co-workers

GS12. give clear instructions to specialists/vendors/users/clients as required

GS13. keep stakeholders informed about progress

GS14. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required

GS15. receive and make phone calls, including call forward, call hold, and call mute

GS16. follow rule-based decision-making processes

GS17. make a decision on a suitable course of action

GS18. plan and organize your work to achieve targets and deadlines

GS19. Identify internal or external customer requirement and priorities clearly with respect to work at hand

GS20. carry out rule-based transactions in line with customer-specific guidelines, procedures, rules and service level agreements

GS21. check that your own and/or your peers work meets customer requirements

GS22. apply problem-solving approaches in different situations

GS23. seek clarification on problems from others

GS24. analyze data and activities

GS25. configure data and disseminate relevant information to others

GS26. pass on relevant information to others

GS27. provide opinions on work in a detailed and constructive way

GS28. apply balanced judgments to different situations

GS29. check your work is complete and free from errors

GS30. work effectively in a team environment

GS31. work independently and collaboratively

GS32. assess the robustness of security systems and designs

GS33. evaluate the adequacy of security designs

GS34. use network analysis tools to identify vulnerabilities

GS35. develop and deploy signatures custom tools/scripts with the help of various scripting languages like ShellScript, Python, Perl or Ruby and write exploits using programming languages like C

GS36. collect data from a variety of computer network defense resources

GS37. work on various operating system

GS38. work with word processers, spreadsheets and presentations

GS39. perform basic penetration testing and ethical hacking

GS40. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	30	**70**	**-**	**-**
PC1. Consult with customers to evaluate functional requirements for network security.	1	3	-	-
PC2. Define project scope and objectives based on customer requirements.	1	3	-	-
PC3. Confirm the availability of complete and accurate details of the security objectives.	1	2	-	-
PC4. Review the usage of existing network security measures, and assess risks w.r.t security objectives.	2	2	-	-
PC5. create documents using standard templates and agreed language standards	2	2	-	-
PC6. Consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements.	1	3	-	-
PC7. Conduct technical risk analysis, threat identification of the existing network security measures	2	3	-	-
PC8. Identify the level of risk acceptable for business requirements by discussing with business and technical leads	1	3	-	-
PC9. Critically interpret information and data, from both within the customer/client organization and other sources, in order to identify network security requirements.	1	3	-	-
PC10. Research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks	1	3	-	-
PC11. Identify and record details of constraints that may have an impact on the business and security options.	1	2	-	-
PC12. Explore potential vulnerabilities that could be technical, operational or management related .	1	4	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC13. Categorize vulnerabilities and identify the extent of vulnerability including the level of weakness and sensitivity of the information .	1	3	-	-
PC14. Identify the root cause of vulnerabilities.	1	3	-	-
PC15. Research options of network security solutions that match the productivity and security requirements captured .	1	4	-	-
PC16. Gather sufficient accurate information on which to determine potential costs, benefits , and effectiveness of potential security solutions .	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 .	1	2	-	-
PC18. Prepare recommendations that have the potential to meet the security objectives of the organization.	1	3	-	-
PC19. Provide details of costs, benefits, effectiveness, limitations , and constraints of recommendations	1	2	-	-
PC20. Provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales .	1	2	-	-
PC21. Provide the organization with considered advice on the implications of accepting, modifying or rejecting security recommendations .	1	2	-	-
PC22. Co ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs .	1	3	-	-
PC23. Take account of the organizations values, culture , and nature of the business .	1	2	-	-
PC24. Maintain the security and confidentiality of information relating to your organization and recommendations.	1	2	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC25. Obtain necessary approvals from the responsible persons as per organizational policy.	1	2	-	-
PC26. Evaluate ways & means of closing weaknesses in the network.	1	3	-	-
PC27. Maintain logs for all the activities performed	1	2	-	-
NOS Total	**30**	**70**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0925
NOS Name	Test, run exploits to identify vulnerabilities in networks
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	7
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0927: Drive interrelated cyber security actions

Description

This unit is about working with different teams to drive interrelated cyber security actions.

Scope

This unit/task covers the following:Cyber security functions and operations:

- vulnerability scanning
- threat management
- security monitoring and incident management
- security governance
- risk and compliance management
- security policy management
- security review and audit
- application security
- access and identity management
- endpoint securityKey Cyber security activities are: e.g.
- vulnerability scanning
- threat management
- security monitoring and incident management
- security governance
- risk and compliance management
- security policy management
- security review and audit
- application security
- access and identity management
- endpoint security, etc.Operating procedures include:
- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentialityBasic Cyber security concepts are: e.g.
- the importance of confidentiality, integrity and availability for informationsystems;
- common types of malicious code like o virus o Trojan o logic bomb o worm o spyware
- types of threats facing the information security of individuals and organisations;
- sources of threats to information security in terms of opportunity, ability andmotive, etc.Security solutions:
- Firewall
- IDS/IPS
- web security gateways
- email security

- content management

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. identify the business functions, and key stakeholders within these, and establish their interest and understanding, relevant to achieving the organisation's aims

PC2. recognise the roles, responsibilities, interests and concerns of the stakeholders in other business functions

PC3. identify all the activities, functions and operations that are attributed to security or require analysis from security perspective

PC4. create an inventory of roles that are responsible, accountable and informed for activities, functions and operations in cyber security

PC5. create an inventory of cyber security operations that fall into various key cyber security activities

PC6. identify functions that have a joint working relationship with own function

PC7. consider implication of own work on other functions

PC8. discuss and consult with stakeholders from other functions in relation to key decisions and activities impacting them

PC9. take agreements and track actionables of other functions for interrelated work

PC10. follow up with appropriate personnel for meeting timelines and effective functioning

PC11. agree on communication and documentation process with stakeholders and maintain the same

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

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

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

PC15. undertake actions agreed with stakeholders in line with the terms of any agreements made

PC16. advise stakeholders of difficulties or where it will be impossible to fulfil agreed actions in line with the terms of any agreements made

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company including cyber security policy

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. the operating procedures that are applicable to the system(s) being used

KU6. typical response times and service times related to own work area

KU7. different business functions and their roles and responsibilities in achieving the organizations overall aims function

KU8. basic cyber security concepts

KU9. information assurance (IA) principles

KU10. various cyber security functions and operations

KU11. cyber security roles and responsibilities

KU12. the enterprise information technology (IT) architecture Information technology architecture

KU13. measures or indicators of system performance and availability Information

KU14. functions that can be impacted by own work

KU15. activities that will need joint working

KU16. various stakeholders to own work in other functions

KU17. internet ports, protocols and services and their usefulness

KU18. security solutions

KU19. the reasons why there may be conflicts and misunderstandings between business functions, for example, regarding which publics/stakeholders and activities are the most important

KU20. why it is important to identify key colleagues and stakeholders within the different business functions

KU21. principles of effective communication and how to apply them in order tocommunicate effectively with colleagues and stakeholders

KU22. why it is important to recognize the roles, responsibilities, interests and concerns of colleagues and stakeholders

KU23. how to consult with colleagues and stakeholders in relation to key decisions and activities

KU24. importance of taking account of the views of colleagues and stakeholders, particularly in relation to their priorities, expectations and attitudes towards the role of the marketing

KU25. why communication with colleagues and stakeholders on fulfilment of agreements or any problems affecting or preventing fulfilment is important

KU26. how to identify conflicts of interest with colleagues and stakeholders and the techniques that can be used to manage or remove them

KU27. importance of agreeing upon communication and documentation strategy for joint working

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. document call logs, reports, task lists, and schedules with co-workers

GS2. prepare status and progress reports

GS3. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes

GS4. read about new products and services with reference to the organization and also from external forums such as websites and blogs

GS5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets

GS6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal

GS7. read policy manual, standard operating procedures and service level agreements relevant to work area

GS8. read emails received from own team, across team and external vendors and clients

GS9. discuss task lists, schedules, and work-loads with co-workers

GS10. give clear instructions to specialists/vendors/users/clients as required

GS11. keep stakeholders informed about progress

GS12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required

GS13. receive and make phone calls, including call forward, call hold, and call mute

GS14. follow rule-based decision-making processes

GS15. make decisions on suitable courses of action

GS16. plan and organize your work to achieve targets and deadlines

GS17. carry out rule-based transactions in line with customer-specific guidelines,

GS18. procedures, rules and service level agreements

GS19. check your own and/or your peers work meets customer requirements

GS20. apply problem-solving approaches in different situations

GS21. seek clarification on problems from others

GS22. analyze data and activities

GS23. configure data and disseminate relevant information to others

GS24. pass on relevant information to others

GS25. provide opinions on work in a detailed and constructive way

GS26. apply balanced judgments to different situations

GS27. apply good attention to details

GS28. check your work is complete and free from errors

GS29. work effectively in a team environment

GS30. contribute to the quality of team working

GS31. work independently and collaboratively

GS32. work on various operating systems

GS33. work with word processors, spreadsheets and presentations

GS34. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

GS35. track deliverables and follow up with stakeholders

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	35	**65**	**-**	**-**
PC1. identify the business functions, and key stakeholders within these, and establish their interest and understanding, relevant to achieving the organisation's aims	-	4	-	-
PC2. recognise the roles, responsibilities, interests and concerns of the stakeholders in other business functions	3	3	-	-
PC3. identify all the activities, functions and operations that are attributed to security or require analysis from security perspective	-	4	-	-
PC4. create an inventory of roles that are responsible, accountable and informed for activities, functions and operations in cyber security	3	4	-	-
PC5. create an inventory of cyber security operations that fall into various key cyber security activities	3	4	-	-
PC6. identify functions that have a joint working relationship with own function	-	4	-	-
PC7. consider implication of own work on other functions	2	5	-	-
PC8. discuss and consult with stakeholders from other functions in relation to key decisions and activities impacting them	2	5	-	-
PC9. take agreements and track actionables of other functions for interrelated work	3	4	-	-
PC10. follow up with appropriate personnel for meeting timelines and effective functioning	3	5	-	-
PC11. agree on communication and documentation process with stakeholders and maintain the same	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	2	3	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
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	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	2	5	-	-
PC15. undertake actions agreed with stakeholders in line with the terms of any agreements made	3	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	3	4	-	-
NOS Total	**35**	**65**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0927
NOS Name	Drive interrelated cyber security actions
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information and Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N0928: Manage a project team

Description

This unit is about managing a team working on a project.

Scope

This unit/task covers the following:Operating procedures includes:

- required service levels (e.g. availability, quality)
- routine maintenance
- monitoring
- data integrity (e.g. backups, anti-virus)
- consumables use, storage & disposal
- health & safety
- escalation
- information recording and reporting
- obtaining work permissions
- security & confidentiality

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives

PC2. brief team members on the project and their work allocations

PC3. inform team members of changes to work allocations in an appropriate way

PC4. provide appropriate support and guidance to team members

PC5. monitor and assess the performance of the team against agreed objectives and work plans

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

PC7. take effective action to manage any actual or potential conflict between team members

PC8. update objectives and work plans regularly, to take account of any individual, team and organisational changes

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. relevant legislation, standards, policies, and procedures followed in the company

KU2. organizations knowledge base and how to access and update this

KU3. limits of your role and responsibilities and who to seek guidance from

KU4. the organizational systems, procedures and tasks/checklists within the domain and how to use these

KU5. the operating procedures that are applicable to the system(s) being used

KU6. typical response times and service times related to own work area
KU7. relevant legislative, regulatory and organizational requirements
KU8. the context of the project
KU9. the arrangements for the delivery of the project
KU10. relevant management plans for the project team
KU11. methods for monitoring and evaluating progress
KU12. how to allocate and authorize project work
KU13. how to communicate team and individual responsibilities clearly to those involved
KU14. how to manage conflict between team members
KU15. the application of negotiation and influencing skills
KU16. the differences between managing individuals for whom you have
KU17. managerial responsibility and those who you do not, and the implications this difference may have for project management

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. document call logs, reports, task lists, and schedules with co-workers
GS2. prepare status and progress reports
GS3. write memos and e-mail to customers, co-workers, and vendors to provide them with work updates and to request appropriate information without English language errors regarding grammar or sentence construct and following professional etiquettes
GS4. read about new products and services with reference to the organization and also from external forums such as websites and blogs
GS5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets
GS6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal
GS7. read policy manual, standard operating procedures and service level agreements relevant to work area
GS8. read emails received from own team, across team and external vendors and clients
GS9. discuss task lists, schedules, and work-loads with co-workers
GS10. give clear instructions to specialists/vendors/users/clients as required
GS11. keep stakeholders informed about progress
GS12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required
GS13. receive and make phone calls, including call forward, call hold, and call mute
GS14. follow rule-based decision-making processes
GS15. make a decision on a suitable course of action
GS16. plan and organize your work to achieve targets and deadlines
GS17. carry out rule-based transactions in line with customer-specific guidelines,
GS18. procedures, rules and service level agreements

GS19. check your own and/or your peers work meets customer requirements
GS20. apply problem-solving approaches in different situations
GS21. seek clarification on problems from others
GS22. analyze data and activities
GS23. configure data and disseminate relevant information to others
GS24. pass on relevant information to others
GS25. provide opinions on work in a detailed and constructive way
GS26. apply balanced judgments to different situations
GS27. use information technology effectively, to make tracker, charts and reports
GS28. Use various modes of communication which working with the project team including but not limited to conference calls, group messaging, web conferences, video conferences, group sharing and working on documents on cloud, etc.
GS29. keep up to date with changes, procedures and practices in your role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	32	**68**	**-**	**-**
PC1. ensure the allocation and authorisation of work to the project management team is consistent with achieving the project objectives	3	9	-	-
PC2. brief team members on the project and their work allocations	3	9	-	-
PC3. inform team members of changes to work allocations in an appropriate way	3	9	-	-
PC4. provide appropriate support and guidance to team members	5	9	-	-
PC5. monitor and assess the performance of the team against agreed objectives and work plans	5	8	-	-
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	4	8	-	-
PC7. take effective action to manage any actual or potential conflict between team members	4	8	-	-
PC8. update objectives and work plans regularly, to take account of any individual, team and organisational changes	5	8	-	-
NOS Total	**32**	**68**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0928
NOS Name	Manage a project team
Sector	IT-ITeS
Sub-Sector	IT Services
Occupation	Information/Cyber Security
NSQF Level	8
Credits	NA
Version	1.0
Last Reviewed Date	31/03/2018
Next Review Date	31/03/2022
NSQC Clearance Date	NA

SSC/N9001: Manage your work to meet requirements

Description

This unit is about planning and organizing your work in order to complete it to the required standards on time.

Scope

The scope covers the following :

- Utilise resources
- Ensure compliance

Elements and Performance Criteria

To be competent, the user/individual on the job must be able to:

PC1. establish and agree your work requirements with appropriate people
PC2. keep the immediate work area clean and tidy
PC3. utilize time effectively
PC4. use resources correctly and efficiently
PC5. treat confidential information correctly
PC6. work in line with the organization's policies and procedures
PC7. work within the limits of the job role
PC8. obtain guidance from appropriate people, where necessary
PC9. ensure the work meets the agreed requirements

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. the priorities for the area of work
KU2. role, responsibilities, limits of the responsibilities and whom these must be agreed with, as well as when to involve others
KU3. the importance of having a tidy work area and how to do this
KU4. how to prioritize your workload according to urgency and importance and the benefits of this
KU5. the organizations policies and procedures, especially for dealing with confidential information, and the importance of complying with these
KU6. the purpose of keeping others updated with the progress of the work
KU7. the purpose and value of being flexible and adapting work plans to reflect change
KU8. the importance of completing work accurately and how to do this
KU9. appropriate timescales for completing the work and the implications of not meeting these for self and the organization
KU10. resources needed for the work and how to obtain and use these

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. read instructions, guidelines, procedures, rules and service level agreements
GS2. ask for clarification and advice from line managers
GS3. communicate orally with colleagues
GS4. make decisions on suitable courses
GS5. plan and organize the work to achieve targets and deadlines
GS6. agree to objectives and work requirements
GS7. deliver consistent and reliable service to customers
GS8. check that the work meets customer requirements
GS9. refer anomalies to the line manager
GS10. seek clarification on problems from others
GS11. provide relevant information to others
GS12. analyze needs, requirements and dependencies in order to meet the work requirements
GS13. apply judgments to different situations
GS14. ensure the work is complete and free from errors
GS15. get the work checked by peers
GS16. work effectively in a team environment
GS17. use information technology effectively, to input and/or extract data accurately
GS18. identify and refer anomalies in data
GS19. store and retrieve information
GS20. keep up to date with changes, procedures and practices in the role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
	25	**75**	**-**	**-**
PC1. establish and agree your work requirements with appropriate people	-	6.25	-	-
PC2. keep the immediate work area clean and tidy	6.25	6.25	-	-
PC3. utilize time effectively	6.25	6.25	-	-
PC4. use resources correctly and efficiently	6.25	12.5	-	-
PC5. treat confidential information correctly	-	6.25	-	-
PC6. work in line with the organization's policies and procedures	-	12.5	-	-
PC7. work within the limits of the job role	-	6.25	-	-
PC8. obtain guidance from appropriate people, where necessary	-	6.25	-	-
PC9. ensure the work meets the agreed requirements	6.25	12.5	-	-
NOS Total	**25**	**75**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9001
NOS Name	Manage your work to meet requirements
Sector	IT-ITeS
Sub-Sector	IT Services, Business Process Management, Engineering R&D, Software Product Development, IT Support Services, Software Products, Future Skills
Occupation	Generic
NSQF Level	4
Credits	TBD
Version	2.0
Last Reviewed Date	16/08/2019
Next Review Date	22/09/2025
NSQC Clearance Date	22/09/2020

SSC/N9002: Work effectively with colleagues

Description

This unit is about working effectively with colleagues, either in your own work group or in other work groups within your organization.

Scope

The scope covers the following :

- Communicate with colleagues
- Show respect

Elements and Performance Criteria

Communicate with colleagues

To be competent, the user/individual on the job must be able to:

PC1. communicate with colleagues clearly, concisely and accurately

PC2. work with colleagues to integrate the work effectively with theirs

PC3. pass on essential information to colleagues in line with organizational requirements

Show respect

To be competent, the user/individual on the job must be able to:

PC4. work in ways that show respect for colleagues

PC5. carry out commitments one has made to colleagues

PC6. identify any problems while working with colleagues and take the initiative to solve these problems

PC7. follow the organization’s policies and procedures for working with colleagues

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. the organization's policies and procedures for working with colleagues and the role and responsibilities in relation to this

KU2. the importance of effective communication and establishing good working relationships with colleagues

KU3. different methods of communication and the circumstances in which it is appropriate to use these

KU4. benefits of developing productive working relationships with colleagues

KU5. the importance of creating an environment of trust and mutual respect in an environment where there is no authority over those working with

KU6. where you do not meet the commitments, the implications this will have on individuals and the organization

KU7. different types of information that colleagues might need and the importance of providing this information when it is required

KU8. the importance of understanding problems from the colleagues perspective and how to provide support, where necessary, to resolve these

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate, well written work with attention to detail
GS2. communicate effectively with colleagues in writing
GS3. read instructions, guidelines, procedures, rules and service level agreements
GS4. make decisions on suitable courses
GS5. ask for clarification and advice from line managers
GS6. help reach agreements with colleagues
GS7. plan and organize the work to achieve targets and deadlines
GS8. ensure the work meets customer requirements, and deliver consistent and reliable service
GS9. apply problem solving approaches in different situations
GS10. apply balanced judgments to different situations
GS11. ensure the work is complete and free from errors
GS12. ensure the work is complete and free from errors
GS13. work effectively with colleagues and other teams in a team environment
GS14. treat other cultures with respect
GS15. identify and refer anomalies
GS16. keep up to date with changes, procedures and practices in the role

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Communicate with colleagues	**18**	**30**	**-**	**-**
PC1. communicate with colleagues clearly, concisely and accurately	-	20	-	-
PC2. work with colleagues to integrate the work effectively with theirs	-	10	-	-
PC3. pass on essential information to colleagues in line with organizational requirements	18	-	-	-
Show respect	**2**	**50**	**-**	**-**
PC4. work in ways that show respect for colleagues	2	20	-	-
PC5. carry out commitments one has made to colleagues	-	10	-	-
PC6. identify any problems while working with colleagues and take the initiative to solve these problems	-	10	-	-
PC7. follow the organization's policies and procedures for working with colleagues	-	10	-	-
NOS Total	**20**	**80**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9002
NOS Name	Work effectively with colleagues
Sector	IT-ITeS
Sub-Sector	IT Services, Business Process Management, Engineering R&D, Software Product Development, IT Support Services, Software Products, Future Skills
Occupation	Generic
NSQF Level	4
Credits	TBD
Version	2.0
Last Reviewed Date	16/08/2019
Next Review Date	22/09/2025
NSQC Clearance Date	22/09/2020

SSC/N9004: Provide data/information in standard formats

Description

This unit is about providing specified data/information related to your work in templates or other standard formats.

Scope

The scope covers the following :

- Obtain information
- Analyze and report information

Elements and Performance Criteria

Obtain information

To be competent, the user/individual on the job must be able to:

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

PC2. obtain the data/information from reliable sources

PC3. check that the obtained data/information is accurate, complete and up-to-date

PC4. obtain advice or guidance from appropriate people where there are problems with the data/information

Analyze and report information

To be competent, the user/individual on the job must be able to:

PC5. carry out rule-based analysis of the data/information, if required

PC6. insert the data/information into the agreed formats

PC7. report any unresolved anomalies in the data/ information to appropriate people

PC8. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. the organization's procedures and guidelines for providing data/information in standard formats and the role and responsibilities in relation to this

KU2. the knowledge management culture of the organization

KU3. the organization's policies and procedures for recording and sharing information and the importance of complying with these

KU4. the importance of validating data/information before use and how to do this

KU5. procedures for updating data in appropriate formats and with proper validation

KU6. the purpose of the CRM database

KU7. how to use the CRM database to record and extract information

KU8. the importance of having data/information reviewed by others
KU9. the scope of any data/information requirements including the level of detail required
KU10. the importance of keeping within the scope of work and adhering to timescales
KU11. data/information one may need to provide including the sources and how to do this
KU12. templates and formats used for data/information including their purpose and how to use these
KU13. different techniques used to obtain data/information and how to apply these
KU14. rule-based analysis on the data/information
KU15. typical anomalies that may occur in data/information
KU16. whom to go to in the event of inaccurate data/information and how to report this

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. complete accurate, well written work with attention to detail
GS2. read instructions, guidelines, procedures, rules and service level agreements
GS3. listen effectively and orally communicate information accurately
GS4. follow rule-based decision-making processes
GS5. make decisions on suitable courses of action
GS6. plan and organize the work to achieve targets and deadlines
GS7. check the work meets customer requirements and exceed customer expectations
GS8. apply problem solving approaches in different situations
GS9. configure data and disseminate relevant information to others
GS10. apply balanced judgments to different situations
GS11. use information technology effectively, to input and/or extract data accurately
GS12. validate and update data
GS13. store and retrieve information

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Obtain information	**18.75**	**31.25**	**-**	**-**
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	12.5	-	-	-
PC2. obtain the data/information from reliable sources	-	12.5	-	-
PC3. check that the obtained data/information is accurate, complete and up-to-date	6.25	6.25	-	-
PC4. obtain advice or guidance from appropriate people where there are problems with the data/information	-	12.5	-	-
Analyze and report information	**6.25**	**43.75**	**-**	**-**
PC5. carry out rule-based analysis of the data/information, if required	-	25	-	-
PC6. insert the data/information into the agreed formats	-	12.5	-	-
PC7. report any unresolved anomalies in the data/ information to appropriate people	6.25	-	-	-
PC8. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time	-	6.25	-	-
NOS Total	**25**	**75**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9004
NOS Name	Provide data/information in standard formats
Sector	IT-ITeS
Sub-Sector	IT Services, Business Process Management, Engineering R&D, Software Product Development, IT Support Services, Software Products, Future Skills
Occupation	Generic
NSQF Level	4
Credits	TBD
Version	2.0
Last Reviewed Date	31/03/2020
Next Review Date	22/09/2025
NSQC Clearance Date	22/09/2020

SSC/N9014: Maintain an inclusive, environmentally sustainable workplace

Description

The unit is about implementing and improving diversity equality and inclusion in a sustainable and environment friendly workplace.

Scope

The scope covers the following :

- Sustainable Practices
- Respect diversity and strengthen practices to promote equity (equality)/inclusivity

Elements and Performance Criteria

Sustainable Practices

To be competent, the user/individual on the job must be able to:

PC1. optimize usage of electricity/energy, materials, and water in various asks / activities / processes and plan the implementation of energy efficient systems in a phased manner

PC2. segregate recyclable, non-recyclable and hazardous waste generated for disposal or efficient waste management

Respect diversity and strengthen practices to promote equity (equality)/inclusivity

To be competent, the user/individual on the job must be able to:

PC3. understand the diversity policy of the organization and use internal & external communication to colleagues to improve

PC4. comply with PwD inclusive policies for an adaptable and equitable work environment

PC5. improve through specifically designed recruitment practices, PwD friendly infrastructure, job roles, etc.

PC6. use and advocate for appropriate verbal/nonverbal communication, schemes and benefits of PwD.

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. the organization's policies and procedures about gender inclusivity, equality and sustainability while working with colleagues and your role and responsibilities in relation to this

KU2. inclusive tools and practices of communication to acknowledge/validate, share and promote the cause of gender parity at workplace. For example - supporting women with mentorship programs, speaking out against discriminatory practices or harassment

KU3. the concept of gender, gender equality and gender discrimination, and all forms of gender discrimination, violence and inequality, including the current and historical causes of gender inequality in the workplace

KU4. how to maintain and provide a conducive work environment that is free from any harassment. facilities and amenities to PwD to perform and excel in their role

KU5. organization's redressal mechanisms (like the POSH committee) to address harassment and bias at the workplace, with awareness of prevalent legislations against bias and sexual harassment

KU6. initiatives towards efficient use of natural resources and energy, reduction and prevention of pollution and promoting waste avoidance and recycling measures in line with internationally disseminated technologies and practices

KU7. all about various energy options including renewable and non-renewable with their environmental impacts, health issues, usage, safety and energy security

KU8. implications that any non-compliance with electricity and energy may have on individuals and the organization

KU9. the organization's electricity first aid emergency procedures

KU10. how to monitor, measure and report performance of environmental conservation

KU11. different types of electricity accidents, safety and security and how and when to report these

KU12. how to use the electricity/energy safety, accident reporting, emergency procedures and the importance of these

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. read PwD instructions, guidelines, procedures, diversity policies/acts, rules and service level agreements

GS2. be aware of one's own gender identity and gender role.and respectful of the gender performances of others

GS3. organize team building or sensitization workshops to address gender biases, stereotypes and potentially blind spots

GS4. clarify personal norms and values related to energy production and usage as well as to reflect and evaluate their own energy usage in terms of efficiency and sufficiency

GS5. listen and communicate (oral) effectively and accurately on all PwD policies

GS6. apply balanced judgments in gender diversity situations

GS7. take action to reduce the carbon footprint of business activities and embed environmental responsibility

GS8. calibration session with employees to discuss gender biases, stereotypes and potentially blind spots

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Sustainable Practices	**10**	**30**	**-**	**-**
PC1. optimize usage of electricity/energy, materials, and water in various asks / activities / processes and plan the implementation of energy efficient systems in a phased manner	5	15	-	-
PC2. segregate recyclable, non-recyclable and hazardous waste generated for disposal or efficient waste management	5	15	-	-
Respect diversity and strengthen practices to promote equity (equality)/inclusivity	**10**	**50**	**-**	**-**
PC3. understand the diversity policy of the organization and use internal & external communication to colleagues to improve	5	10	-	-
PC4. comply with PwD inclusive policies for an adaptable and equitable work environment	-	10	-	-
PC5. improve through specifically designed recruitment practices, PwD friendly infrastructure, job roles, etc.	-	20	-	-
PC6. use and advocate for appropriate verbal/nonverbal communication, schemes and benefits of PwD.	5	10	-	-
NOS Total	**20**	**80**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9014
NOS Name	Maintain an inclusive, environmentally sustainable workplace
Sector	IT-ITeS
Sub-Sector	IT Services, Business Process Management, Engineering R&D, Software Product Development, Future Skills
Occupation	Generic,
NSQF Level	5
Credits	TBD
Version	1.0
Last Reviewed Date	27/01/2022
Next Review Date	27/01/2027
NSQC Clearance Date	22/09/2020

Assessment Guidelines and Assessment Weightage

Assessment Guidelines

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 subsequent assessment on the balance NOS's to pass the Qualification Pack.

Minimum Aggregate Passing % at QP Level : 70

(**Please note**: Every Trainee should score a minimum aggregate passing percentage as specified above, to

successfully clear the Qualification Pack assessment.)

Assessment Weightage

Compulsory NOS

National Occupational Standards	Theory Marks	Practical Marks	Project Marks	Viva Marks	Total Marks	Weightage
SSC/N0918.Maintain compliance to information security policies, regulations and standards andaddress risk issues	32	68	-	-	100	12
SSC/N0922.Provide network security recommendations as per requirements	32	68	-	-	100	12
SSC/N0923.Carry out configuration review and provide recommendations for secure configuration of networks and security devices	32	68	-	-	100	12
SSC/N0925.Test, run exploits to identify vulnerabilities in networks	30	70	-	-	100	12
SSC/N0927.Drive interrelated cyber security actions	35	65	-	-	100	12
SSC/N0928.Manage a project team	32	68	-	-	100	12
SSC/N9001.Manage your work to meet requirements	25	75	-	-	100	8
SSC/N9002.Work effectively with colleagues	20	80	-	-	100	8
SSC/N9004.Provide data/information in standard formats	25	75	-	-	100	8

National Occupational Standards	Theory Marks	Practical Marks	Project Marks	Viva Marks	Total Marks	Weightage
SSC/N9014.Maintain an inclusive, environmentally sustainable workplace	20	80	-	-	100	4
Total	**283**	**717**	**-**	**-**	**1000**	**100**

Acronyms

NOS	National Occupational Standard(s)
NSQF	National Skills Qualifications Framework
QP	Qualifications Pack
TVET	Technical and Vocational Education and Training
IT-ITeS	Information Technology - Information Technology enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	Legal Process Outsourcing
IPO	Information Process Outsourcing
BCA	Bachelor of Computer Applications
B.Sc	. Bachelor of Science
B.Sc	Bachelor of Science
IT-ITeS	Information Technology - Information Technology enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	Legal Process Outsourcing
IPO	Information Process Outsourcing
IT-ITeS	Information Technology - Information Technology Enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	Legal Process Outsourcing
IPO	Information Process Outsourcing

IT-ITeS	Information Technology - Information Technology enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	Legal Process Outsourcing
IPO	Information Process Outsourcing
IT-ITeS	Information Technology - Information Technology enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	LPO
IPO	Information Process Outsourcing

Glossary

Sector	Sector is a conglomeration of different business operations having similar business and interests. It may also be defined as a distinct subset of the economy whose components share similar characteristics and interests.
Sub-sector	Sub-sector is derived from a further breakdown based on the characteristics and interests of its components.
Occupation	Occupation is a set of job roles, which perform similar/ related set of functions in an industry.
Job role	Job role defines a unique set of functions that together form a unique employment opportunity in an organisation.
Occupational Standards (OS)	OS specify the standards of performance an individual must achieve when carrying out a function in the workplace, together with the Knowledge and Understanding (KU) they need to meet that standard consistently. Occupational Standards are applicable both in the Indian and global contexts.
Performance Criteria (PC)	Performance Criteria (PC) are statements that together specify the standard of performance required when carrying out a task.
National Occupational Standards (NOS)	NOS are occupational standards which apply uniquely in the Indian context.
Qualifications Pack (QP)	QP comprises the set of OS, together with the educational, training and other criteria required to perform a job role. A QP is assigned a unique qualifications pack code.
Unit Code	Unit code is a unique identifier for an Occupational Standard, which is denoted by an 'N'
Unit Title	Unit title gives a clear overall statement about what the incumbent should be able to do.
Description	Description gives a short summary of the unit content. This would be helpful to anyone searching on a database to verify that this is the appropriate OS they are looking for.
Scope	Scope is a set of statements specifying the range of variables that an individual may have to deal with in carrying out the function which have a critical impact on quality of performance required.
Knowledge and Understanding (KU)	Knowledge and Understanding (KU) are statements which together specify the technical, generic, professional and organisational specific knowledge that an individual needs in order to perform to the required standard.

Organisational Context	Organisational context includes the way the organisation is structured and how it operates, including the extent of operative knowledge managers have of their relevant areas of responsibility.
Technical Knowledge	Technical knowledge is the specific knowledge needed to accomplish specific designated responsibilities.
Core Skills/ Generic Skills (GS)	Core skills or Generic Skills (GS) are a group of skills that are the key to learning and working in today's world. These skills are typically needed in any work environment in today's world. These skills are typically needed in any work environment. In the context of the OS, these include communication related skills that are applicable to most job roles.
Electives	Electives are NOS/set of NOS that are identified by the sector as contributive to specialization in a job role. There may be multiple electives within a QP for each specialized job role. Trainees must select at least one elective for the successful completion of a QP with Electives.
Options	Options are NOS/set of NOS that are identified by the sector as additional skills. There may be multiple options within a QP. It is not mandatory to select any of the options to complete a QP with Options.
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk.
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk.
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk.
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk.