QUALIFICATIONS PACK – NATIONAL OCCUPATIONAL STANDARDS FOR IT-BPM INDUSTRY

Contents

What are National Occupational Standards(NOS)?

- NOS describe what individuals need to do, know and understand in order to carry out a particular job role or function
- NOS are performance standards that individuals must achieve when carrying out functions in the workplace, together with specifications of the underpinning knowledge and understanding

Contact Us:

IT-ITeS SSC NASSCOM
Plot No -7,8.9 & 10 ,
Sector 126 , Noida ,
UP.Noida : 201303
Phone No: 01204990172

E-mail:
ssc@nasscom.in

Introduction

Qualifications Pack- Forensics Specialist

SECTOR: IT-ITeS

SUB-SECTOR: IT Services

OCCUPATION: Information/Cyber Security

REFERENCE ID: SSC/Q0922

ALIGNED TO: NCO-2004/NIL

Forensic Specialist: in some organisations Forensic Specialist is known as Forensic Consultant.

Brief Job Description: The main duties consist of identifying, preserving and seizing digital/electronic forensic evidences, extracting information and data from the digital information or data sources or devices, examining and analyzing the information or data and further reporting and presenting the findings before competent authority.

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, passion for information security and attention for detail. The individual should also be ethical, compliance and result oriented, should also be able to demonstrate interpersonal skills, along with willingness to undertake desk-based job with long working hours.

Job Details

Qualifications Pack Code	**SSC/Q0922**		
Job Role	**Forensic Specialist** **This job role is applicable in both national and international scenarios**		
Credits (NSQF)	**TBD**	**Version number**	**1.0**
Sector	**IT-ITeS**	**Drafted on**	**18/08/2016**
Sub-sector	**IT Services**	**Last reviewed on**	**18/08/2016**
Occupation	**Information/Cyber Security**	**Next review date**	**18/08/2017**
NSQC Clearance on	**DD/MM/2016**		

Job Role	**Forensic Specialist**
Role Description	Is responsible for identifying, seizing evidences, examining and anlysing the data and information and presenting the results in a forensically sound manner before competent authority.
NSQF level	8
Minimum Educational Qualifications	Graduate in Security/ Computer Science/Electronics and Engineering /Information Technology
Maximum Educational Qualifications	NA
Training (Suggested but not mandatory)	Certification in Information systems or related fields, Basic soft skills training, ethical hacking or pertaining to ISO27001
Minimum Job Entry Age	23 years
Experience	2-5 years of work experience/internship in information technology
Applicable National Occupational Standards (NOS)	**Compulsory:** **1.** SSC/N0929 Identify, preserve, and seize digital/electronic devices or records for investigation of possible breach or crime **2.** SSC/N0930 Extract relevant data or information from digital/electronic forensic evidences **3.** SSC/N0931 Analyze information or data extracted from digital/electronic forensic evidences **4.** SSC/N0932 Report and present the results of a forensic investigation **5.** SSC/N9001 Manage your work to meet requirements **6.** SSC/N9002 Work effectively with colleagues **7.** SSC/N9003 Maintain a healthy, safe and secure working environment **8.** SSC/N9004 Provide data/information in standard formats **9.** SSC/N9005 Develop your knowledge, skills and competence **Optional:** Not Applicable
Performance Criteria	As described in the relevant OS units

Glossary of Key Terms

Definitions

Keywords /Terms	Description
Core Skills/Generic Skills	Core Skills or Generic Skills are a group of skills that are key to learning and working in today's world. These skills are typically needed in any work environment. In the context of the NOS, these include communication related skills that are applicable to most job roles.
Function	Function is an activity necessary for achieving the key purpose of the sector, occupation, or area of work, which can be carried out by a person or a group of persons. Functions are identified through functional analysis and form the basis of NOS.
Job role	Job role defines a unique set of functions that together form a unique employment opportunity in an organization.
Knowledge and Understanding	Knowledge and Understanding are statements which together specify the technical, generic, professional and organizational specific knowledge that an individual needs in order to perform to the required standard.
National Occupational Standards (NOS)	NOS are Occupational Standards which apply uniquely in the Indian context
Occupation	Occupation is a set of job roles, which perform similar/related set of functions in an industry.
Organizational Context	Organizational Context includes the way the organization is structured and how it operates, including the extent of operative knowledge managers have of their relevant areas of responsibility.
Performance Criteria	Performance Criteria are statements that together specify the standard of performance required when carrying out a task.
Qualifications Pack(QP)	Qualifications Pack comprises the set of NOS, together with the educational, training and other criteria required to perform a job role. A Qualifications Pack is assigned a unique qualification pack code.
Qualifications Pack Code	Qualifications Pack Code is a unique reference code that identifies a qualifications pack.
Scope	Scope is the 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 the quality of performance required.
Sector	Sector is a conglomeration of different business operations having similar businesses 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.
Sub-functions	Sub-functions are sub-activities essential to fulfil the achieving the objectives of the function.
Technical Knowledge	Technical Knowledge is the specific knowledge needed to accomplish specific designated responsibilities.
Unit Code	Unit Code is a unique identifier for a NOS unit, which can be denoted with an 'N'
Unit Title	Unit Title gives a clear overall statement about what the incumbent should be able to do.

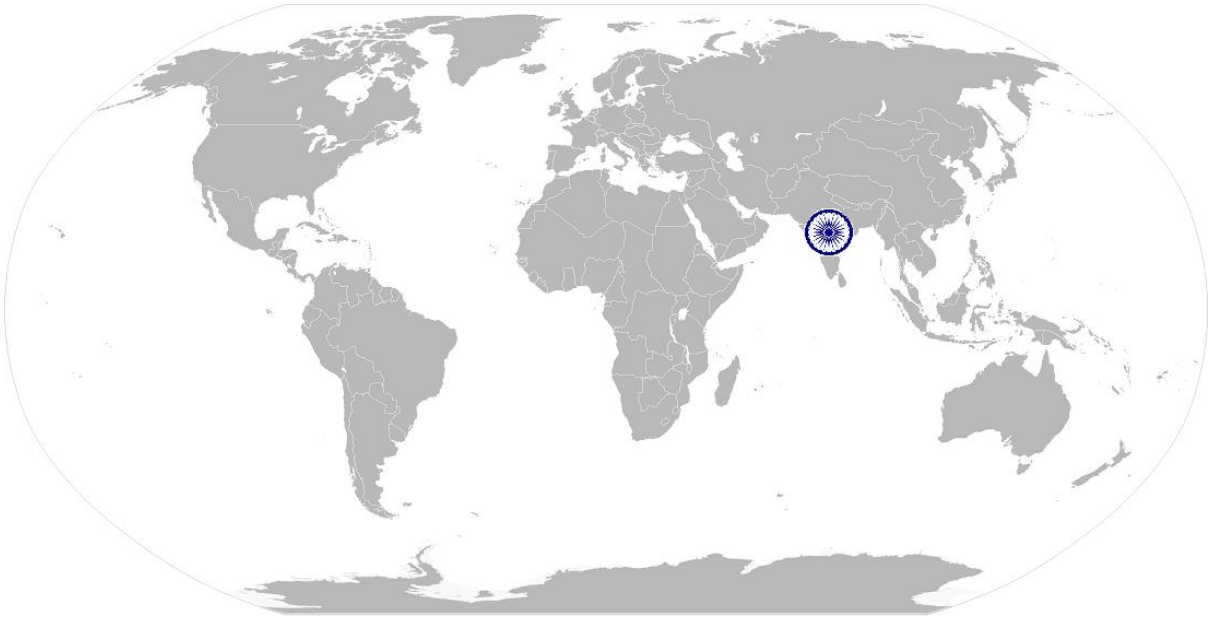
Acronyms

Vertical	Vertical may exist within a sub-sector representing different domain areas or the client industries served by the industry.

Keywords /Terms	Description
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
OS	Occupational Standard(s)
NOS	National Occupational Standard(s)
QP	Qualifications Pack
UGC	University Grants Commission
MHRD	Ministry of Human Resource Development
MoLE	Ministry of Labour and Employment
NVEQF	National Vocational Education Qualifications Framework
NVQF	National Vocational Qualifications Framework
NSQF	National Skill Qualification Framework

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

National Occupational Standard



Overview

This unit is about Identifying and seizing computing devices or records for investigation of possible breach or crime.

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

National Occupational Standard

Unit Code	SSC/N0929
Unit Title (Task)	Identify and seize computing devices or records for investigation of possible breach or crime
Description	This unit is about Identifying and seizing computing devices or records for investigation of possible breach or crime.
Scope	This unit/task covers the following: **Authorisations:** • contract • due diligence • consent • legal order by competent authority **Necessary resources:** • backup devices • blank media • evidence handling supplies, etc. (e.g., hard-bound notebooks, chain of custody forms, evidence storage bags and tags, evidence tape, digital cameras) • ensure power supply continuation • Cyber forensic tools to collect volatile/non-volatile data **Sources of data:** • With internal drives (e.g. desktop computers, servers, network storage devices, laptops); • external storage forms (e.g. thumb drives, memory and flash cards, optical discs, and magnetic disks); • portable digital devices (e.g., PDAs, cell phones, digital cameras, digital recorders, audio players); etc. **Other sources:** • network activity logs; • application usage data; • logs generated by security monitoring controls such as intrusion detection software, antivirus software, and spyware detection and removal utilities; keystroke monitoring; etc. **Relevant information:** • passwords • phone numbers

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

- URLs
- user account details
- open encrypted volumes
- information stored remotely

Packages:

- faraday bag
- box
- opaque
- anti-static covers

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

System files:

- log files
- registry files
- configuration files

Common Cyber security solutions: e.g.

- firewall
- IDS/IPS
- web security gateways
- email security
- content management, etc.

Performance Criteria(PC) w.r.t. the Scope

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

Element	Performance Criteria
	To be competent, you must be able to: PC1. ensure that necessary **authorisations** and **resources** are in place to conduct a forensics evidence seizure for an investigation PC2. ensure that the scene is physically secured to prevent unauthorized access and alteration or damage of the evidence as per containment policies and situational considerations PC3. survey a physical area and identify potential **sources of data** that could be evidence PC4. identify **other sources** of data and the owner of the same that can be accessed PC5. identify and obtain materials related to digital communications which are **relevant** to the investigation PC6. Ensure identified device or component is up and running however is being disconnected from any network PC7. check for and terminate any destructive software running on any device while seeking to save as much information as possible PC8. estimate the relative likely value of each potential data source for the investigation PC9. identify whether data in the device or record is volatile or non-volatile so that both types of data can be adequately preserved PC10. create a plan that prioritizes the sources, establishing the order in which the computing devices or records can be acquired PC11. use forensic tools to collect volatile data PC12. duplicate non-volatile data sources to collect their data, securing the original non-volatile data sources PC13. verify and preserve the integrity of the data source device or record in accordance with investigation procedures PC14. record current state, condition and configuration of digital devices and media and potentially relevant information at the time of seizure PC15. handle digital devices and media consistent with preserving other potential evidence sources including fingerprints or DNA PC16. document any activity on the computer, components, or devices by taking photographs or recording any information that may be relevant PC17. maintain a detailed log of every step that was taken to collect the data, including information about each tool used in the process and handlers PC18. photograph and label the components of the device making specific reference to ancillary leads and connections to the device

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

	PC19. appropriately **package**, seal and label the device in accordance with current diligence procedures PC20. check packaging of forensic items in line with forensic procedures, and identify, record and address any packaging problems PC21. carefully document each stage of the seizure and investigation PC22. ensure chain of custody is followed for all digital media acquired in accordance with the rules of evidence PC23. identify any risks to safety linked to working with forensic items in line with health and safety procedures PC24. take the necessary actions to minimise any risks linked to working with forensic items PC25. transport and store forensic items to relevant authorities in line with investigative procedures, and in a way that avoids risk to potential evidence, including loss, breakage, contamination, cross-contamination, degradation, etc. PC26. record details of the storage, handling, transfer and packaging of forensic items in line with organisational procedures
Knowledge and Understanding (K)	
A. Organizational Context (Knowledge of the company / organization and its processes)	You need to know and understand: KA1. relevant legislation, policies, procedures, codes of practice, guidelines and applicable standards for seizing and recording electronic evidence sources KA2. organization's knowledge base and how to access and update this KA3. limits of your role and responsibilities and who to seek guidance from KA4. the organizational systems, procedures and tasks/checklists within the domain and how to use these KA5. the **operating procedures** that are applicable to the system(s) being used KA6. typical response times and service times related to own work area
B. Technical Knowledge	You need to know and understand: KB1. types of electronic evidence, devices containing electronic evidence and external connections to such devices KB2. possible electronic evidence sources KB3. processes for seizing and preserving digital evidence and maintaining chain of custody KB4. methods of protecting and concealing electronic information including locking, encryption, sealing, etc. KB5. how to identify and deal with protected and/or concealed systems KB6. the types of operating systems and how to deal with them KB7. which **system files** contain relevant information and where to find those

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

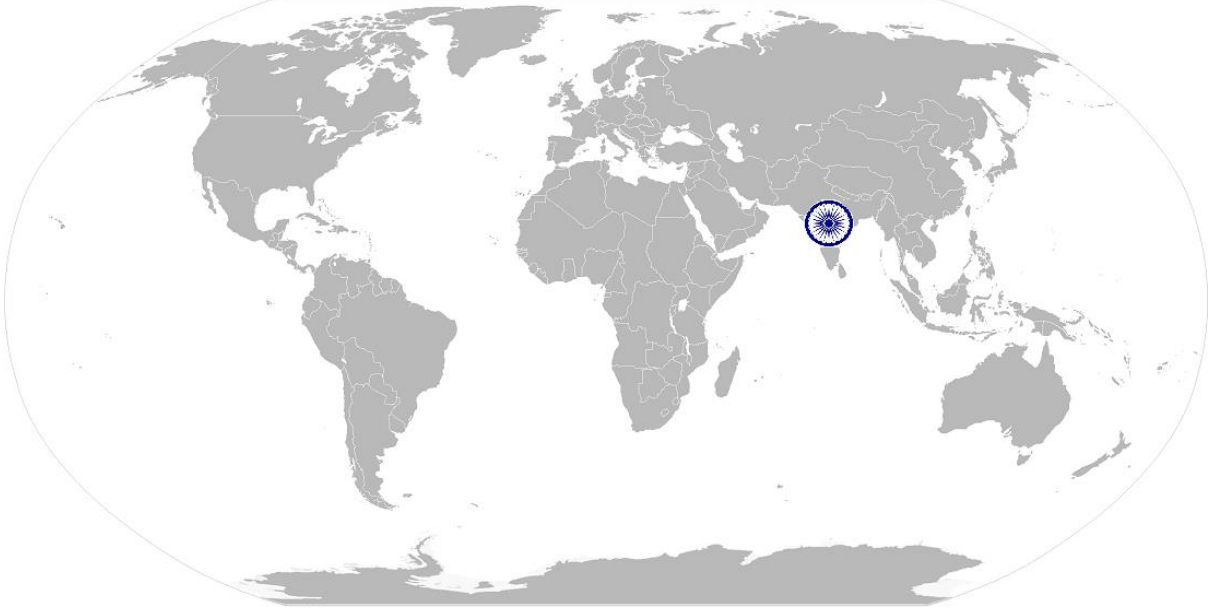
	system files KB8. how to preserve the information on battery powered devices KB9. the types of actions necessary to preserve third party and volatile data sources KB10. do's and don'ts for seizing and recording electronic evidence sources KB11. how to keep a record of the seizure process, the condition and state of the device and the reasons why this is important KB12. knowledge of all aspects of the computer including but not limited to hard drives, networking, and encryption KB13. the impact of actions on victims and witnesses KB14. the importance of considering all potentially relevant information in the immediate vicinity KB15. the actions necessary to safeguard the device for forensic examinations KB16. how to conduct a preview of the contents of electronic devices KB17. the need to consider physical forensic examinations and the implications KB18. the importance of maintaining an accurate contemporaneous record using appropriate methods KB19. processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data KB20. handling memory forensics and volatile evidences KB21. importance of crime scene management and what does it entail KB22. internet ports, protocols and services and their usefulness KB23. **Common cyber security solutions** KB24. work on various operating systems
Skills (S)	
A. Core Skills/ Generic Skills	**Writing Skills**
	You need to know and understand how to: SA1. document call logs, reports, task lists, and schedules with co-workers SA2. prepare status and progress reports SA3. 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
	Reading Skills
	You need to know and understand how to: SA4. read about new products and services with reference to the organization and also from external forums such as websites and blogs SA5. keep abreast with the latest knowledge by reading brochures, pamphlets, and

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

	product information sheets SA6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal SA7. read policy manual, standard operating procedures and service level agreements relevant to work area SA8. read emails received from own team, across team and external vendors and clients
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA9. discuss task lists, schedules, and work-loads with co-workers SA10. give clear instructions to specialists/vendors/users/clients as required SA11. keep stakeholders informed about progress SA12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required SA13. receive and make phone calls, including call forward, call hold, and call mute
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. follow rule-based decision-making processes SB2. make decisions on suitable courses of action
	Plan and Organize
	You need to know and understand how to: SB3. plan and organize your work to achieve targets and deadlines
	Customer Centricity
	You need to know and understand how to: SB3. carry out rule-based transactions in line with customer-specific guidelines, SB4. procedures, rules and service level agreements SB5. check your own and/or your peers work meets customer requirements
	Problem Solving
	You need to know and understand how to: SB6. apply problem-solving approaches in different situations SB7. seek clarification on problems from others
	Analytical Thinking
	You need to know and understand how to: SB8. analyze data and activities SB9. configure data and disseminate relevant information to others SB10. pass on relevant information to others
	Critical Thinking

SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

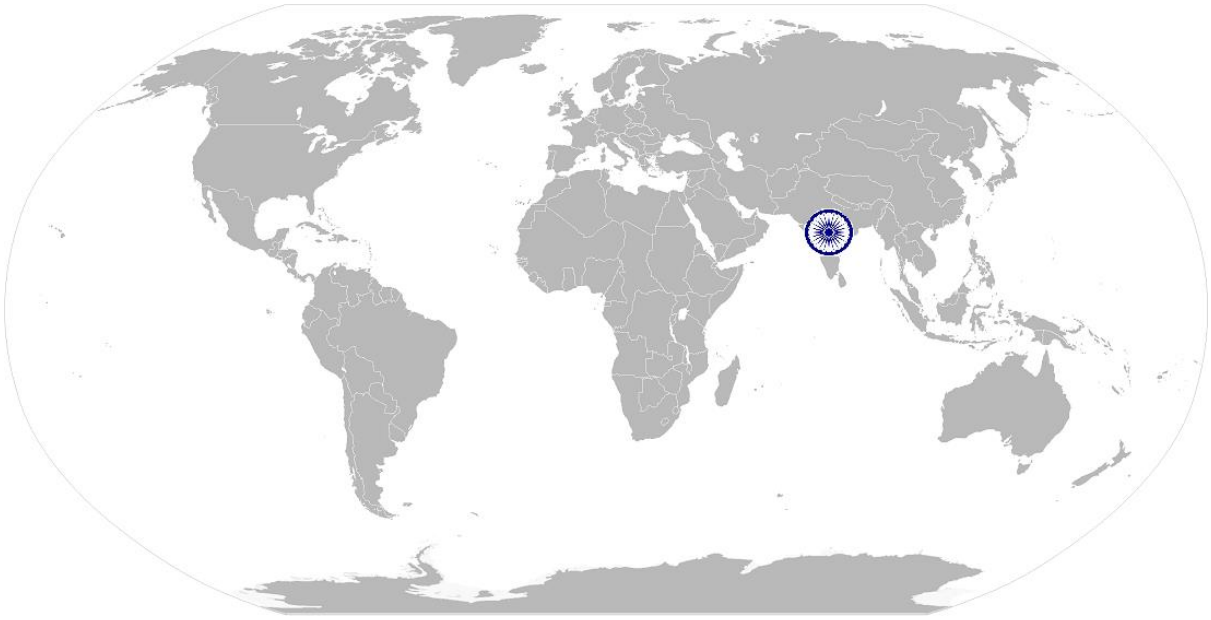
	You need to know and understand how to: SB11. provide opinions on work in a detailed and constructive way SB12. apply balanced judgments to different situations
C. Technical Skills	You need to know and understand how to: SC1. analyze the system architecture and design SC2. evaluate operating system and file system configurations SC3. configure networking and security devices SC4. manage backups and storages SC5. deploy and configure application systems SC6. use word processors, spreadsheets and presentations SC7. stay abreast of the latest developments as per industry standards and security tools to ensure that corporate security methods and tools



SSC/N0929 Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime

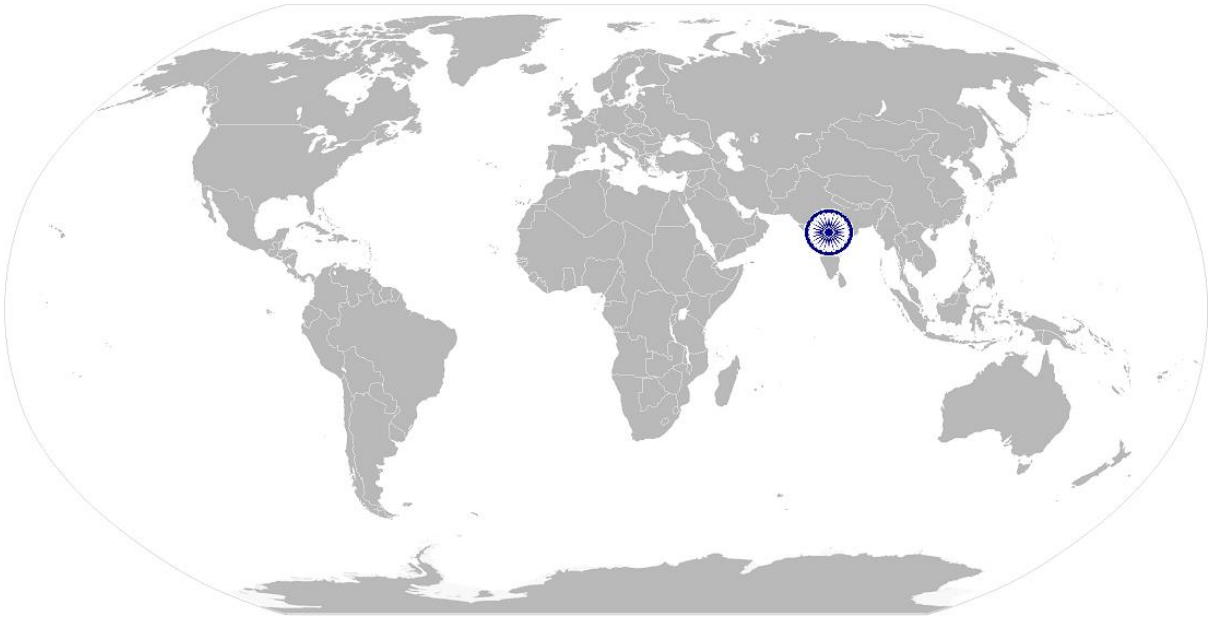
NOS Version Control

NOS Code	SSC/N0929		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	18/08/16
Industry Sub-sector	IT Services	Last reviewed on	18/08/16
Occupation	Information/Cyber Security	Next review date	18/08/17



SSC/N0930 Extract relevant data or information from digital forensic evidences

National Occupational Standard



Overview

This unit is about extracting data or information from the digital forensic evidences collected for the investigation of an information security/cybercrime.

SSC/N0930 Extract relevant data or information from digital forensic evidences

National Occupational Standard

Unit Code	SSC/N0930
Unit Title (Task)	**Extract relevant data or information from digital forensic evidences**
Description	This unit contains the practical competences, knowledge and understanding and skills required for extracting data or information from the digital forensic evidences collected for the investigation of an information security/cybercrime so that the data may be made available for further analysis. This has to be done without contaminating or effecting the data nor physical evidences like DNA, fingerprints, etc.
Scope	This unit/task covers the following: **Necessary resources:** • backup devices • blank media • forensic workstations • isolation chamber • forensic examination tools • evidence handling supplies, etc. (e.g. clean blank media, faraday bags, evidence tags, evidence tape, digital cameras) **Files or electronic data** includes but is not limited to: • internet use history • passwords • word processing and spreadsheet documents • images and other files **Operating procedures:** • 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 **Critical assets:**

SSC/N0930 Extract relevant data or information from digital forensic evidences

	• firewalls • publicly accessible servers **Tools:** • SEM software • NFAT software **Binary analysis tools:** • hexedit • command code xxd • hexdump **Encryption algorithms:** • 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] **Types of backups:** • full • incremental **Security solutions**: • Firewall • IDS/IPS • web security gateways • email security • content management
Performance Criteria(PC) w.r.t. the Scope	
Element	**Performance Criteria**
	To be competent, you must be able to: PC1. obtain items relevant to forensic examinations in line with investigative procedures from authorised channels PC2. check forensic items against records and identify and address any inaccuracies

SSC/N0930 Extract relevant data or information from digital forensic evidences

	PC3. identify and obtain **necessary resources** that could be required for extracting relevant data or information from the evidences PC4. create an image or copy of the original storage device using clean storage media to have a backup PC5. install write blocking software to prevent any change to the data on the device or media PC6. identify data that is required to be extracted and most likely sources PC7. select the best method and tools for extraction as per the make and model of device PC8. locate the required **files and electronic data** manually or using forensic tools PC9. display the contents of slack space with hex editors or special slack recovery tools PC10. hunt for files and information that have been hidden, deleted or lost PC11. identify the type of data stored in many files by looking at their file headers or simple histogram PC12. identify presence of encrypted data or the use of steganography and the feasibility of decryption or extracting embedded data PC13. identify the encryption method by examining the file header, identifying encryption programs installed on the system, or finding encryption keys PC14. extract the embedded data by finding the stego key, or by using brute force and cryptographic attacks to determine a password PC15. crack, disable or bypass passwords placed on individual files, as well as OS passwords using various utilities and techniques PC16. find, recover and copy data from disks that may have been hidden, encrypted or damaged, etc. PC17. uncompress files and read disk images PC18. extract data and metadata from files using forensic toolkits PC19. identify malicious activity against OSs using security applications, such as file integrity checkers and host IDSs, etc. PC20. perform string searches and pattern matching using searching tools that use Boolean, fuzzy logic, synonyms and concepts, stemming, and other search methods PC21. assess and extract network traffic data with the goal of determining what happened and how the organization's systems and networks have been affected PC22. obtain relevant information from ISP and cloud service provider after taking due authorisation from Law Enforcement Authority/Agency PC23. reveal (unlock) digital images that have been altered to mask the identity of a place or person

SSC/N0930 Extract relevant data or information from digital forensic evidences

	PC24. submit the device or original media for physical evidence examination after removing the data PC25. when equipment is damaged, dismantle and rebuild the system in order to recover lost data PC26. carefully document the process followed in extraction as well as the data retrieved PC27. identify and minimise any risks to safety linked to working with forensic items in line with health and safety procedures PC28. take measures to ensure preservation of physical evidence like finger prints, DNA etc. while handling the evidence
Knowledge and Understanding (K)	
A. Organizational Context (Knowledge of the company / organization and its processes)	You need to know and understand: KA1. relevant legislation, standards, policies, and procedures followed in the company KA2. organization's knowledge base and how to access and update this KA3. the organizational systems, procedures and tasks/checklists within the domain and how to use these KA4. the **operating procedures** that are applicable to the system(s) being used or task KA5. organization's network architecture and the IP addresses used by **critical assets** KA6. organization's typical patterns of usage on systems and networks KA7. typical response times and service times related to own work area KA8. limits of own responsibility and level of competence required
B. Technical Knowledge	You need to know and understand: KB1. guidelines and applicable standards for seizing and recording electronic evidence sources KB2. usage of **tools** for gathering and presenting network traffic data and their limitations KB3. networking principles KB4. common network and application protocols and security products KB5. network-based threats and attack methods KB6. network traffic data sources KB7. intrusion detection signature documentation KB8. characteristics and relative value of all network traffic data sources so that relevant data can be located KB9. techniques needed for analyzing data and drawing conclusions KB10. basic steps of the examination and analysis processes KB11. various approaches and tools to examining and analyzing network traffic data

SSC/N0930 Extract relevant data or information from digital forensic evidences

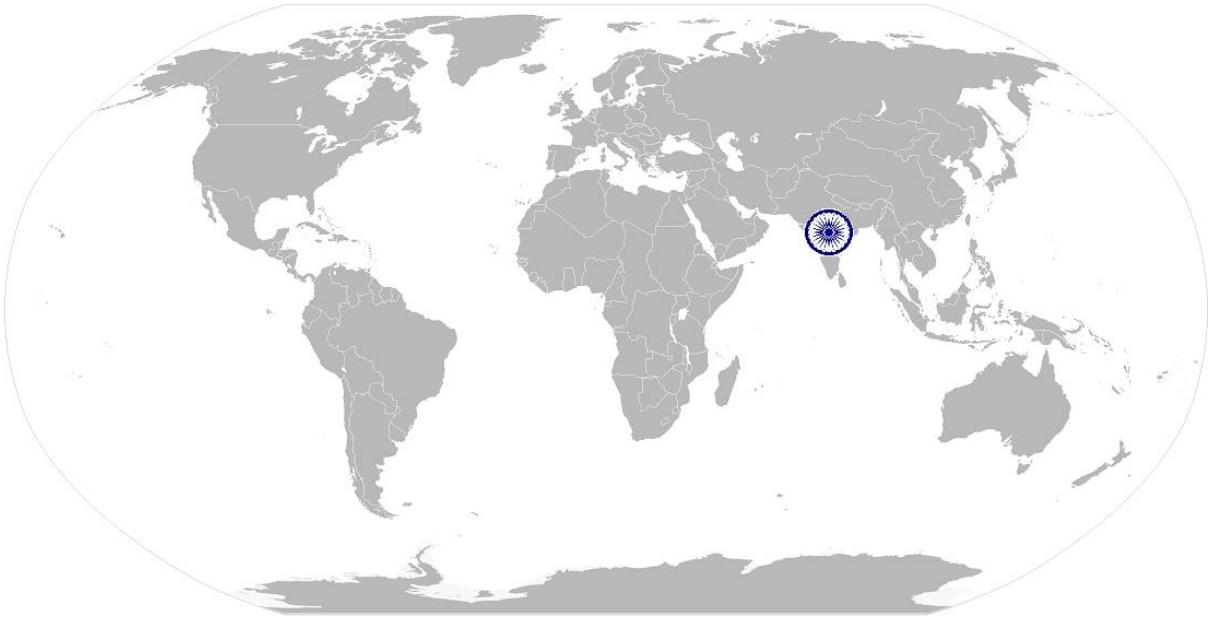
	and their limitations KB12. data carving tools and techniques (e.g., Foremost) KB13. **binary analysis tools** KB14. common **forensic tool configuration and support applications** KB15. debugging procedures and tools KB16. basic concepts and practices of processing digital forensic data KB17. various **encryption algorithms** KB18. how to take data backup or make copies of data sources, **types of backups** KB19. data recovery concepts and tools KB20. server and client operating systems KB21. system and application security threats and vulnerabilities KB22. server diagnostic tools and fault identification techniques KB23. security event correlation tools KB24. malware **analysis tools** KB25. Internet ports, protocols and services and their usefulness KB26. **security solutions**
Skills (S)	
A. Core Skills/ Generic Skills	**Writing Skills**
	You need to know and understand how to: SA1. document call logs, reports, task lists, and schedules with co-workers SA2. prepare status and progress reports SA3. 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
	Reading Skills
	You need to know and understand how to: SA4. read about new products and services with reference to the organization and also from external forums such as websites and blogs SA5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets SA6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal SA7. read policy manual, standard operating procedures and service level agreements relevant to work area SA8. read emails received from own team, across team and external vendors and clients
	Oral Communication (Listening and Speaking skills)

SSC/N0930 Extract relevant data or information from digital forensic evidences

	You need to know and understand how to: SA9. discuss task lists, schedules, and work-loads with co-workers SA10. give clear instructions to specialists/vendors/users/clients as required SA11. keep stakeholders informed about progress SA12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required SA13. receive and make phone calls, including call forward, call hold, and call mute
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. follow rule-based decision-making processes SB2. make decisions on suitable courses of action
	Plan and Organize
	You need to know and understand how to: SB3. plan and organize your work to achieve targets and deadlines
	Customer Centricity
	You need to know and understand how to: SB4. carry out rule-based transactions in line with customer-specific guidelines, SB5. procedures, rules and service level agreements SB6. check your own and/or your peers work meets customer requirements
	Problem Solving
	You need to know and understand how to: SB7. apply problem-solving approaches in different situations SB8. seek clarification on problems from others
	Analytical Thinking
	You need to know and understand how to: SB9. analyze data and activities SB10. configure data and disseminate relevant information to others SB11. pass on relevant information to others
	Critical Thinking
	You need to know and understand how to: SB12. provide opinions on work in a detailed and constructive way SB13. apply balanced judgments to different situations
D. Technical Skills	You need to know and understand how to: SC1. analyze the system architecture and design SC2. evaluate operating system and file system configurations SC3. configure networking and security devices SC4. manage backups and storages SC5. deploy and configure application systems SC6. use word processors, spreadsheets and presentations

SSC/N0930 Extract relevant data or information from digital forensic evidences

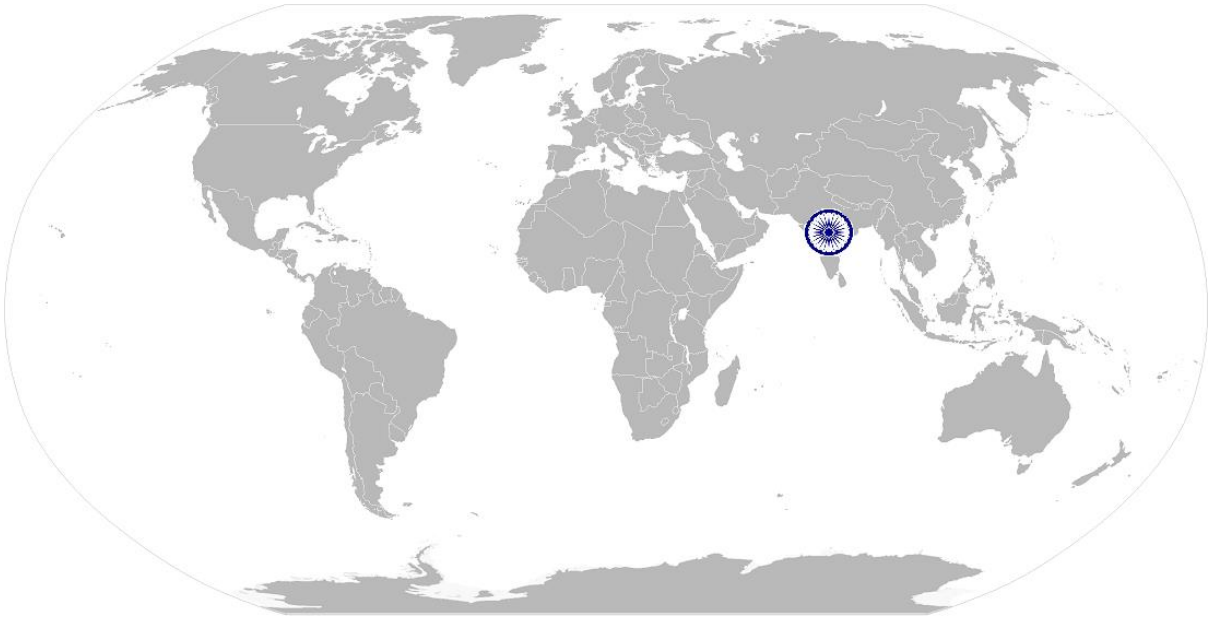
	SC7. stay abreast of the latest developments as per industry standards and security tools to ensure that corporate security methods and tools



SSC/N0930 Extract relevant data or information from digital forensic evidences

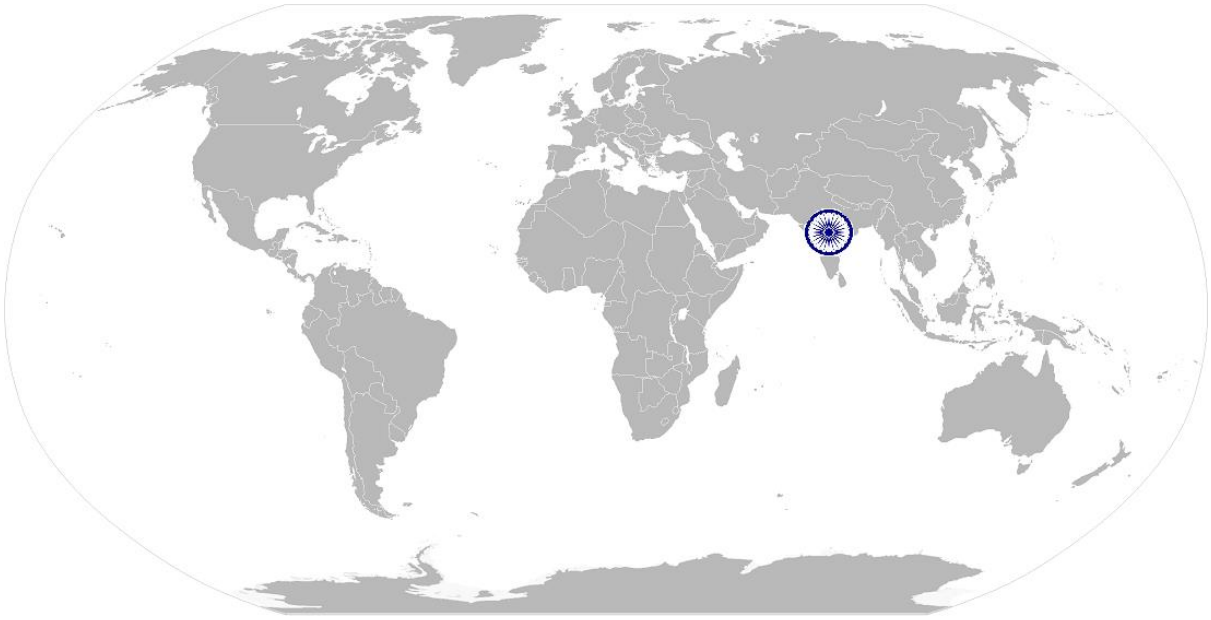
NOS Version Control

NOS Code	SSC/N0930		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	18/08/2016
Industry Sub-sector	IT Services	Last reviewed on	18/08/2016
Occupation	Information/Cyber Security	Next review date	18/08/2017



SSC/N0931 Analyze information or data extracted from digital forensic evidences

National Occupational Standard



Overview

This unit is about for examining and analyzing data or information extracted from the digital forensic evidences.

National Occupational Standard

SSC/N0931 Analyze information or data extracted from digital forensic evidences

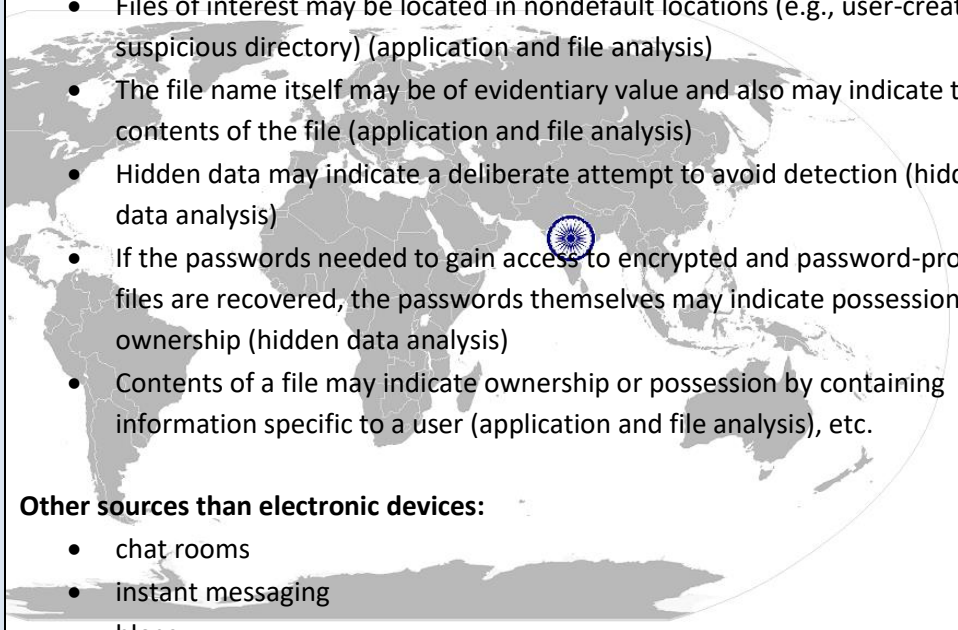
Unit Code	SSC/N0931
Unit Title (Task)	**Analyze information or data extracted from digital forensic evidences**
Description	This unit contains the practical competences, knowledge and understanding and skills required for examining and analyzing data or information extracted from the digital forensic evidences to make inferences about the offender, extent and impact of crime, method used, possible remediation, etc. This has to be done without contaminating or effecting the data nor physical evidences like DNA, fingerprints, etc..
Scope	This unit/task covers the following: **Necessary resources:** • backup devices • blank media • forensic workstations • isolation chamber • forensic examination tools • evidence handling supplies, etc. (e.g. clean blank media, faraday bags, evidence tags, evidence tape, digital cameras) **Forensic tools:** • SEM software • NFAT software • visualization tool **Metadata:** • last modified • last accessed • created • change of status **System and application logs:** • error logs • installation logs • connection logs • security logs **Ways to analyse program and files:** • Reviewing file names for relevance and patterns • Examining file content • Identifying the number and type of operating system(s)

SSC/N0931 Analyze information or data extracted from digital forensic evidences

- Correlating the files to the installed applications
- Considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments
- Identifying unknown file types to determine their value to the investigation
- Examining the users' default storage location(s) for applications and the file structure of the drive to determine if files have been stored in their default or an alternate location(s)
- Examining user-configuration settings

Methods to determine ownership & possession:

- Placing the subject at the computer at a particular date and time may help determine ownership and possession (timeframe analysis)
- Files of interest may be located in nondefault locations (e.g., user-created suspicious directory) (application and file analysis)
- The file name itself may be of evidentiary value and also may indicate the contents of the file (application and file analysis)
- Hidden data may indicate a deliberate attempt to avoid detection (hidden data analysis)
- If the passwords needed to gain access to encrypted and password-protected files are recovered, the passwords themselves may indicate possession or ownership (hidden data analysis)
- Contents of a file may indicate ownership or possession by containing information specific to a user (application and file analysis), etc.



Other sources than electronic devices:

- chat rooms
- instant messaging
- blogs
- websites
- the system of Internet addresses
- email header information
- time stamps on messaging

Various types of forensics analysis include:

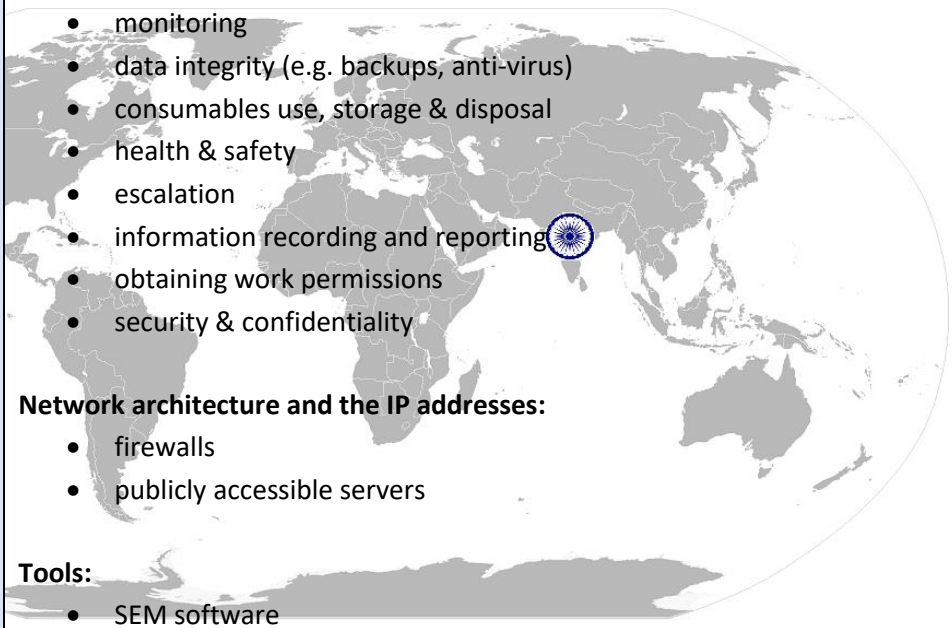
- dynamic analysis to boot an image of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it
- file signature analysis
- file system forensic analysis
- hash comparison against established database

SSC/N0931 Analyze information or data extracted from digital forensic evidences

- live forensic analysis (e.g., using Helix in conjunction with LiveView)
- timeline analysis
- static media analysis
- static analysis to mount an "image" of a drive (without necessarily having the original drive)
- static malware analysis
- tier 1, 2, and 3 malware analysis
- cursory binary analysis

Operating procedures:

- 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 architecture and the IP addresses:

- firewalls
- publicly accessible servers

Tools:

- SEM software
- NFAT software

Binary analysis tools:

- hexedit
- command code xxd
- hexdump

Forensic tool configuration and support applications:

- VMWare
- Wireshark

SSC/N0931 Analyze information or data extracted from digital forensic evidences

	Encryption algorithms: • 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] **Types of backups:** • full • incremental **Security solutions**: • Firewall • IDS/IPS • web security gateways • email security • content management
Performance Criteria(PC) w.r.t. the Scope	
Element	**Performance Criteria**
	To be competent, you must be able to: PC1. identify and obtain **necessary resources** that could be required for examining and analysing of forensic evidences PC2. perform analysis of the extracted data using various **forensic tools** PC3. review the time and date stamps contained in the file system **metadata** to link files of interest to the timeframes relevant to the investigation PC4. review **system and application logs** for relevant information PC5. correlate file headers to the corresponding file extensions to identify any mismatches PC6. perform data hiding analysis for detecting and recovering data and may indicate knowledge, ownership, or intent PC7. **analyse programs and files** in various ways to provide insight into the capability of the system and the knowledge of the user PC8. analyse file metadata typically through the application that created it to provide insight into detailed information like authorship, time last edited, number of times edited, and print or saved location, etc. PC9. determine **ownership and knowledgeable possession** of the questioned data

SSC/N0931 Analyze information or data extracted from digital forensic evidences

	using various methods PC10. analyze network traffic data with the goal of determining what has happened and how the organization's systems and networks have been affected PC11. analyse mobile phone records to trace devices to a particular location (or to rule them out) PC12. follow electronic data trails to uncover links between individuals or groups PC13. piece together strings of interactions that provide a picture of activity using evidence collected from **other sources than electronic devices** PC14. identify additional systems/networks compromised by cyber attacks PC15. identify the most important characteristics of the activity and the negative impact it has caused or may cause the organization PC16. perform computer network defence (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation PC17. perform **various types of forensics analysis** as per the requirement of media type, data or constraints PC18. perform virus scanning on digital media PC19. fuse computer network attack analyses with criminal and counterintelligence investigations and operations PC20. identify elements of proof of the crime PC21. identify outside attackers accessing the system from the internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges PC22. follow investigation procedure in order to determine the identity of attacker PC23. take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations PC24. carefully document each stage of the investigation PC25. identify risks to safety linked to working with forensic items and take the necessary actions to minimise the risks
Knowledge and Understanding (K)	
A. Organizational Context (Knowledge of the company / organization and its processes)	You need to know and understand: KA1. relevant legislation, standards, policies, and procedures followed in the company KA2. organization's knowledge base and how to access and update this KA3. the organizational systems, procedures and tasks/checklists within the domain and how to use these KA4. the **operating procedures** that are applicable to the system(s) being used KA5. organization's **network architecture and the IP addresses** used by critical

SSC/N0931 Analyze information or data extracted from digital forensic evidences

	assets KA6. organization's typical patterns of usage on systems and networks KA7. typical response times and service times related to own work area KA8. limits of own responsibility and level of competence required
B. Technical Knowledge	You need to know and understand: KB1. guidelines and applicable standards for examining and analysing electronic evidence sources KB2. usage of **tools** for gathering and presenting network traffic data and their limitations KB3. networking principles KB4. basic steps of the examination and analysis processes KB5. various analysis approaches and techniques and their application KB6. legal and technical limitations to various analysis approaches and techniques KB7. common network and application protocols and security products KB8. network-based systems and application threats and attack methods KB9. intrusion detection signature documentation KB10. characteristics and relative value of all network traffic data sources so that relevant data can be located KB11. techniques needed for analyzing data and drawing conclusions KB12. data carving tools and techniques (e.g., Foremost) KB13. **binary analysis tools** and their application KB14. common **forensic tool configuration and support applications** KB15. debugging procedures and tools KB16. basic concepts and practices of processing digital forensic data KB17. various **encryption algorithms** KB18. how to take data backup, **types of backups** and recovery concepts and tools KB19. server and client operating systems KB20. server diagnostic tools and fault identification techniques KB21. security event correlation tools KB22. malware **analysis tools** KB23. internet ports, protocols and services and their usefulness KB24. **security solutions**
Skills (S)	
A. Core Skills/	**Writing Skills**

SSC/N0931 Analyze information or data extracted from digital forensic evidences

Generic Skills	You need to know and understand how to: SA1. document call logs, reports, task lists, and schedules with co-workers SA2. prepare status and progress reports SA3. 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
	Reading Skills
	You need to know and understand how to: SA4. read about new products and services with reference to the organization and also from external forums such as websites and blogs SA5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets SA6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal SA7. read policy manual, standard operating procedures and service level agreements relevant to work area SA8. read emails received from own team, across team and external vendors and clients
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA9. discuss task lists, schedules, and work-loads with co-workers SA10. give clear instructions to specialists/vendors/users/clients as required SA11. keep stakeholders informed about progress SA12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required SA13. receive and make phone calls, including call forward, call hold, and call mute
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. follow rule-based decision-making processes SB2. make decisions on suitable courses of action
	Plan and Organize
	You need to know and understand how to: SB3. plan and organize your work to achieve targets and deadlines
	Customer Centricity
	You need to know and understand how to: SB4. carry out rule-based transactions in line with customer-specific guidelines, SB5. procedures, rules and service level agreements

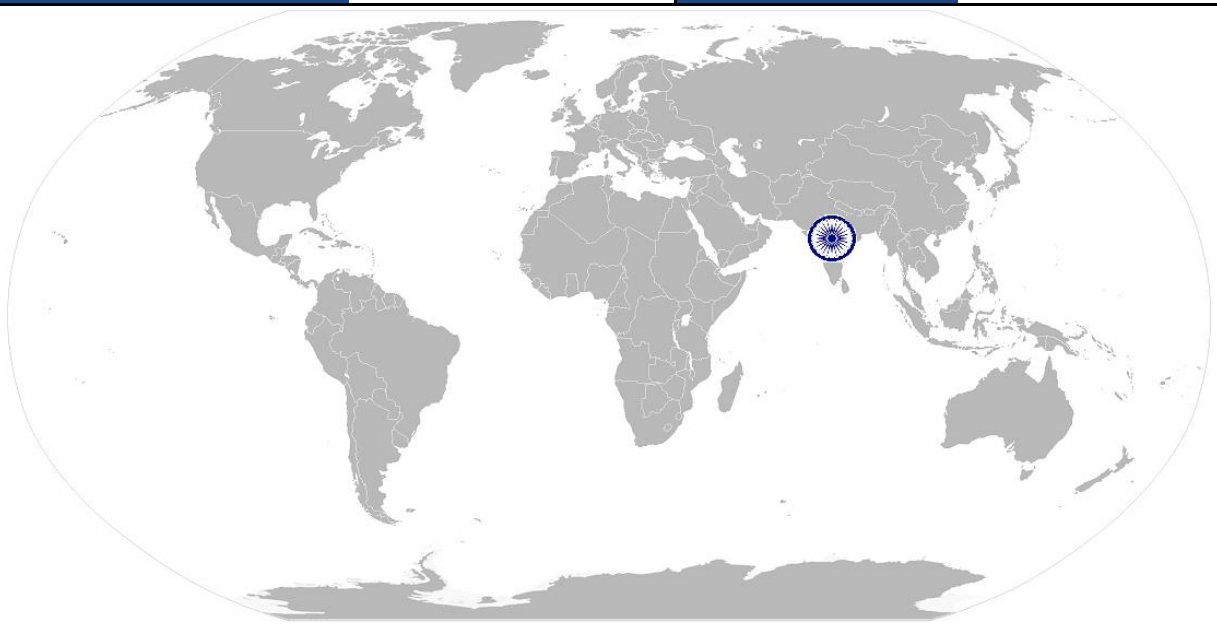
SSC/N0931 Analyze information or data extracted from digital forensic evidences

	SB6. check your own and/or your peers work meets customer requirements
	Problem Solving
	You need to know and understand how to: SB7. apply problem-solving approaches in different situations SB8. seek clarification on problems from others
	Analytical Thinking
	You need to know and understand how to: SB9. analyze data and activities SB10. configure data and disseminate relevant information to others SB11. pass on relevant information to others
	Critical Thinking
	You need to know and understand how to: SB12. provide opinions on work in a detailed and constructive way SB13. apply balanced judgments to different situations
C. Technical Skills	You need to know and understand how to: SC1. analyze the system architecture and design SC2. evaluate operating system and file system configurations SC3. configure networking and security devices SC4. manage backups and storages SC5. deploy and configure application systems SC6. use word processors, spreadsheets and presentations SC7. stay abreast of the latest developments as per industry standards and security tools to ensure that corporate security methods and tools

SSC/N0931 Analyze information or data extracted from digital forensic evidences

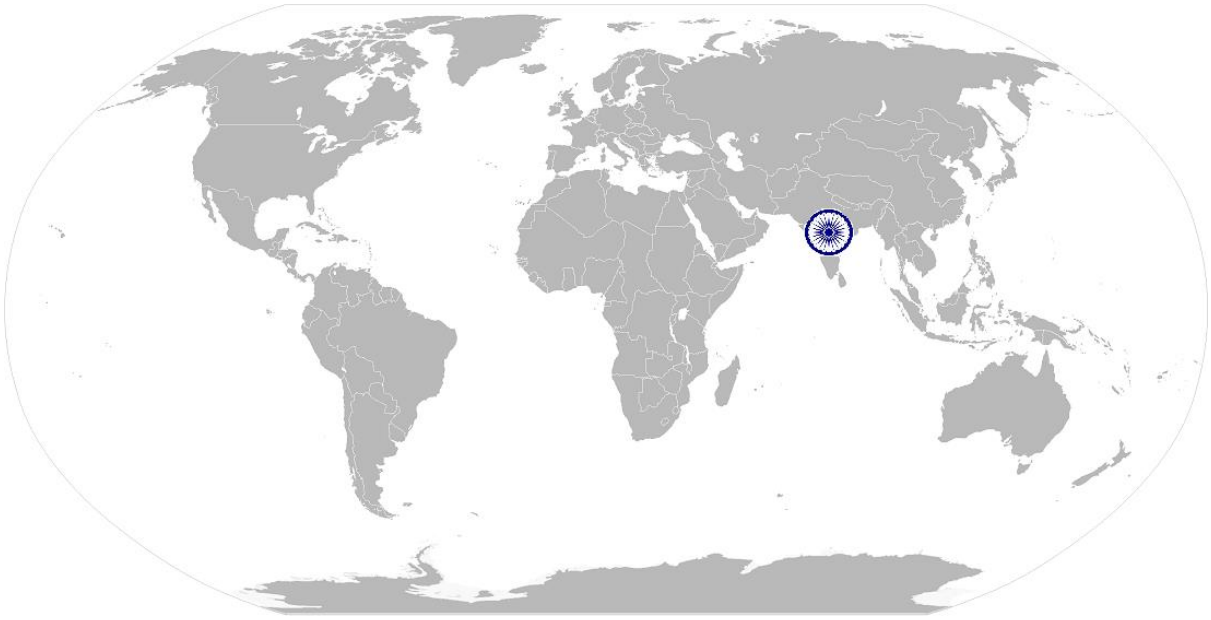
NOS Version Control

NOS Code	SSC/N0931		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	18/08/2016
Industry Sub-sector	IT Services	Last reviewed on	18/08/2016
Occupation	Information/Cyber Security	Next review date	18/08/2017



SSC/N0932 Report and present the results of a forensic investigation

National Occupational Standard



Overview

This unit is about reporting and presenting the results of a forensic investigation.

National Occupational Standard

SSC/N0932 Report and present the results of a forensic investigation

Unit Code	SSC/N0932
Unit Title (Task)	**Report and present the results of a forensic investigation**
Description	This unit contains the practical competences, knowledge and understanding and skills required for reporting and presenting the results of a forensic investigation. This has to be done without contaminating or effecting the data nor physical evidences like DNA, fingerprints, etc..
Scope	This unit/task covers the following: **Necessary resources:** • backup devices • blank media • forensic workstations • isolation chamber • forensic examination tools • evidence handling supplies, etc. (e.g. clean blank media, faraday bags, evidence tags, evidence tape, digital cameras) **Relevant information in the report:** • Identity of the reporting agency • Case identifier or submission number • Case investigator • Identity of the submitter • Date of receipt • Date of report • Descriptive list of items submitted for examination, including serial number, make, and model • Identity and signature of the examiner • Brief description of steps taken during examination, such as string searches, graphics/ image searches, and recovering erased files • Results/conclusions and implications of findings relevant to the case • rationale for examinations • the limitations of examinations undertaken **Comprehensive details may include:** • Specific files related to the request • Other files, including deleted files, that support the findings • String searches, keyword searches, and text string searches

SSC/N0932 Report and present the results of a forensic investigation

	• Internet-related evidence, such as Web site traffic analysis, chat logs, cache files, e-mail, and news group activity • Graphic image analysis • Indicators of ownership, which could include program registration data • Data analysis • Description of relevant programs on the examined items • Techniques used to hide or mask data, such as encryption, steganography, hidden attributes, hidden partitions, and file name anomalies **Operating procedures:** • 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 architecture and the IP addresses:** • firewalls • publicly accessible servers

Performance Criteria(PC) w.r.t. the Scope	
Element	**Performance Criteria**
	To be competent, you must be able to: PC1. identify and obtain **necessary resources** that could be required for reporting and presenting forensic investigation, its results and evidences PC2. ensure all **relevant information** is collated and captured in the report accurately and clearly PC3. list and organise for supporting materials that are included with the report, such as printouts of particular items of evidence, digital copies of evidence, chain of custody documentation, photos, emails (showing email headers, the path and timing emails took to get from source to destination), etc. PC4. create a brief summary of the results of the examinations performed on the items submitted for analysis PC5. provide **comprehensive details** of findings in the report

SSC/N0932 Report and present the results of a forensic investigation

	PC6. create a glossary with the report to assist the reader using an accepted source for the definition of the terms and include appropriate references PC7. ensure that the evidence remains pristine and unaltered while presenting PC8. present and explain track record of information exchange, and the "hash!value", also referred to as a checksum, as a mark of authenticity PC9. carefully document each stage of your investigation PC10. work within the level of authority and expertise taking actions necessary should these be exceeded PC11. differentiate between fact and opinion and express opinions within your area of expertise while writing the report PC12. identify any risks to safety linked to working with forensic items in line with health and safety procedures PC13. take the necessary actions to minimise any risks linked to working with forensic items PC14. take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations PC15. take appropriate action to ensure confidentiality and integrity of report and related documents
Knowledge and Understanding (K)	
A. Organizational Context (Knowledge of the company / organization and its processes)	You need to know and understand: KA1. relevant legislation, standards, policies, and procedures followed in the company KA2. organization's knowledge base and how to access and update this KA3. the organizational systems, procedures and tasks/checklists within the domain and how to use these KA4. the **operating procedures** that are applicable to the system(s) being used KA5. organization's **network architecture and the IP addresses** used by critical assets KA6. organization's typical patterns of usage on systems and networks KA7. typical response times and service times related to own work area KA8. limits of own responsibility and level of competence required
B. Technical Knowledge	You need to know and understand: KB1. the implications of current law, policies, operating procedures and guidelines relevant to the evaluation and interpretation of forensic materials KB2. the type, extent and purpose of reports regarding forensic examinations KB3. the established scientific and forensic principles and practices on which to base conclusions KB4. how to assimilate different opinions and propositions in order to formulate

SSC/N0932 Report and present the results of a forensic investigation

	conclusions within area of expertise KB5. the principles involved in processing, evaluating and interpreting results of examinations, and the importance of considering probability and statistical variation KB6. comparison and evaluation methods and techniques used in forensic examinations KB7. limitations of examinations used, and the importance of expressing these limitations KB8. current opinions on working practice in forensic sampling and evaluation relevant to area of operations KB9. when and how to consider alternative propositions, and how these might be tested KB10. the importance of recognizing the limitations of your own abilities and to consult with others where necessary KB11. how to ensure that information used is current, reliable and accurate KB12. the principal types of stakeholders and their different requirements from forensic examination processes KB13. the importance of communicating to the needs of the audience KB14. methods used to present technical explanations to facilitate KB15. understanding by stakeholders, including non-scientists KB16. methods for checking understanding between relevant parties when communicating KB17. the importance of clarifying areas of agreement and disagreement, and methods for doing this KB18. the importance of impartiality and how to present balanced opinions and conclusions KB19. the importance of ensuring that findings and conclusions you provide are consistent with written reports, statements or other documentation KB20. techniques needed for analyzing data and drawing conclusions KB21. basic steps of the examination and analysis processes KB22. various approaches and tools to examining and analyzing network traffic data and their limitations KB23. basic concepts and practices of processing digital forensic data
Skills (S)	
A. Core Skills/	**Writing Skills**

SSC/N0932 Report and present the results of a forensic investigation

Generic Skills	You need to know and understand how to: SA1. document call logs, reports, task lists, and schedules with co-workers SA2. prepare status and progress reports SA3. 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
	Reading Skills
	You need to know and understand how to: SA4. read about new products and services with reference to the organization and also from external forums such as websites and blogs SA5. keep abreast with the latest knowledge by reading brochures, pamphlets, and product information sheets SA6. read comments, suggestions, and responses to Frequently Asked Questions (FAQs) posted on the helpdesk portal SA7. read policy manual, standard operating procedures and service level agreements relevant to work area SA8. read emails received from own team, across team and external vendors and clients
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA9. discuss task lists, schedules, and work-loads with co-workers SA10. give clear instructions to specialists/vendors/users/clients as required SA11. keep stakeholders informed about progress SA12. avoid using jargon, slang or acronyms when communicating with a customer, unless it is required SA13. receive and make phone calls, including call forward, call hold, and call mute
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. follow rule-based decision-making processes SB2. make decisions on suitable courses of action
	Plan and Organize
	You need to know and understand how to: SB3. plan and organize your work to achieve targets and deadlines
	Customer Centricity

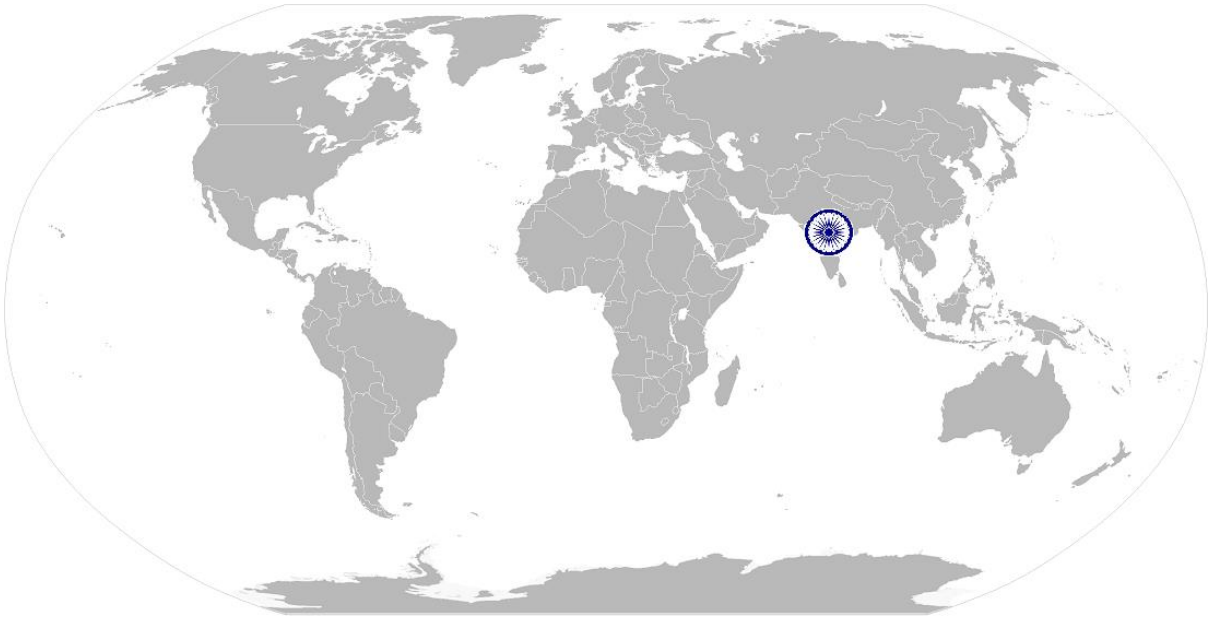
SSC/N0932 Report and present the results of a forensic investigation

	You need to know and understand how to: SB4. carry out rule-based transactions in line with customer-specific guidelines, SB5. procedures, rules and service level agreements SB6. check your own and/or your peers work meets customer requirements
	Problem Solving
	You need to know and understand how to: SB7. apply problem-solving approaches in different situations SB8. seek clarification on problems from others
	Analytical Thinking
	You need to know and understand how to: SB9. analyze data and activities SB10. configure data and disseminate relevant information to others SB11. pass on relevant information to others
	Critical Thinking
	You need to know and understand how to: SB12. provide opinions on work in a detailed and constructive way SB13. apply balanced judgments to different situations
C. Technical Skills	You need to know and understand how to: SC1. work on various operating systems SC2. work with word processors, spreadsheets, presentations and statistical tools SC3. stay abreast of the latest developments in terms of industry standards and information security tools and techniques

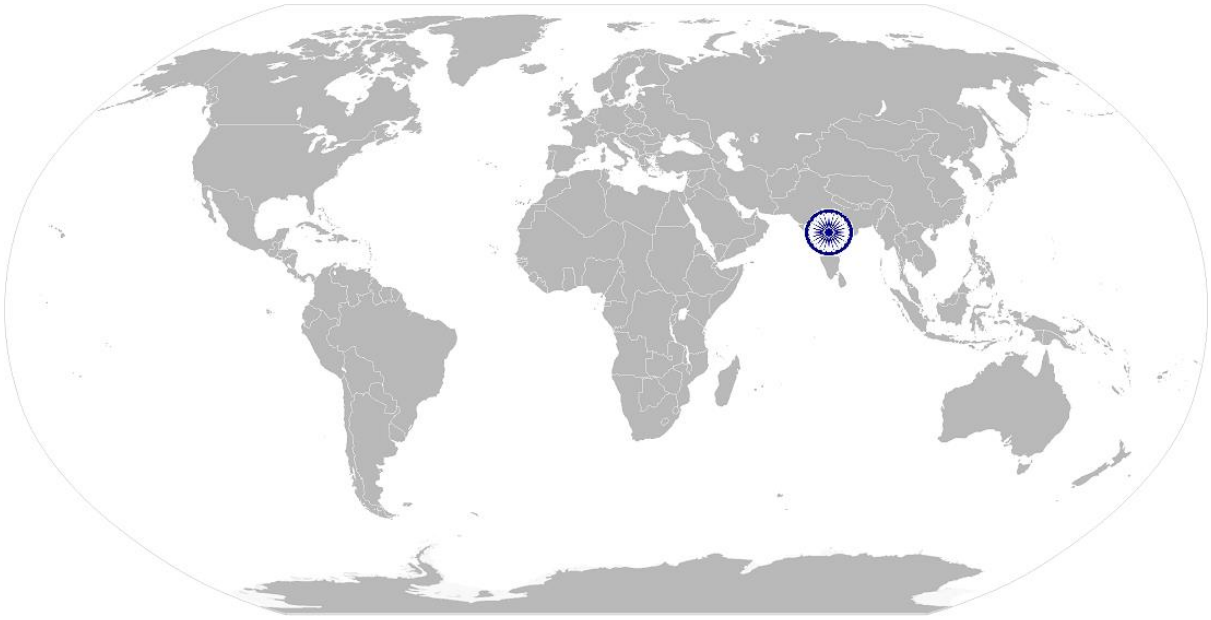
SSC/N0932 Report and present the results of a forensic investigation

NOS Version Control

NOS Code	SSC/N0932		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	18/08/2016
Industry Sub-sector	IT Services	Last reviewed on	18/08/2016
Occupation	Information/Cyber Security	Next review date	18/08/2017



National Occupational Standard



Overview

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

SSC/N9001 Manage your work to meet requirements

Applicable NOS Unit

Unit Code	**SSC/N9001**
Unit Title (Task)	**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	This unit/task covers the following: **Work requirements**: • activities (what you are required to do) • deliverables (the outputs of your work) • quantity (the volume of work you are expected to complete) • standards (what is acceptable performance, including compliance with Service Level Agreements) • timing (when your work needs to be completed) **Appropriate people**: • line manager • the person requesting the work • members of the team/department • members from other teams/departments **Resources**: • equipment • materials • information
Performance Criteria (PC) w.r.t. the Scope	
	To be competent, you 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 organization's 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 (K)	
A. Organizational Context	You need to know and understand: KA1. your organization's policies, procedures and priorities for your area of work

SSC/N9001 **Manage your work to meet requirements**

(Knowledge of the company/ organization and its processes)	and your role and responsibilities in carrying out your work KA2. limits of your responsibilities and when to involve others KA3. your specific work requirements and who these must be agreed with KA4. the importance of having a tidy work area and how to do this KA5. how to prioritize your workload according to urgency and importance and the benefits of this KA6. your organization's policies and procedures for dealing with confidential information and the importance of complying with these KA7. the purpose of keeping others updated with the progress of your work KA8. who to obtain guidance from and the typical circumstances when this may be required KA9. the purpose and value of being flexible and adapting work plans to reflect change
B. Technical Knowledge	You need to know and understand: KB1. the importance of completing work accurately and how to do this KB2. appropriate timescales for completing your work and the implications of not meeting these for you and the organization KB3. resources needed for your work and how to obtain and use these
Skills (S)	
A. Core Skills/ Generic Skills	**Writing Skills**
	You need to know and understand how to: SA1. complete accurate work with attention to detail
	Reading Skills
	You need to know and understand how to: SA2. read instructions, guidelines, procedures, rules and service level agreements
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA3. ask for clarification and advice from line managers SA4. communicate orally with colleagues
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. make a decision on a suitable course of action
	Plan and Organize
	You need to know and understand how to: SB2. plan and organize your work to achieve targets and deadlines SB3. agree objectives and work requirements
	Customer Centricity
	You need to know and understand how to: SB4. deliver consistent and reliable service to customers

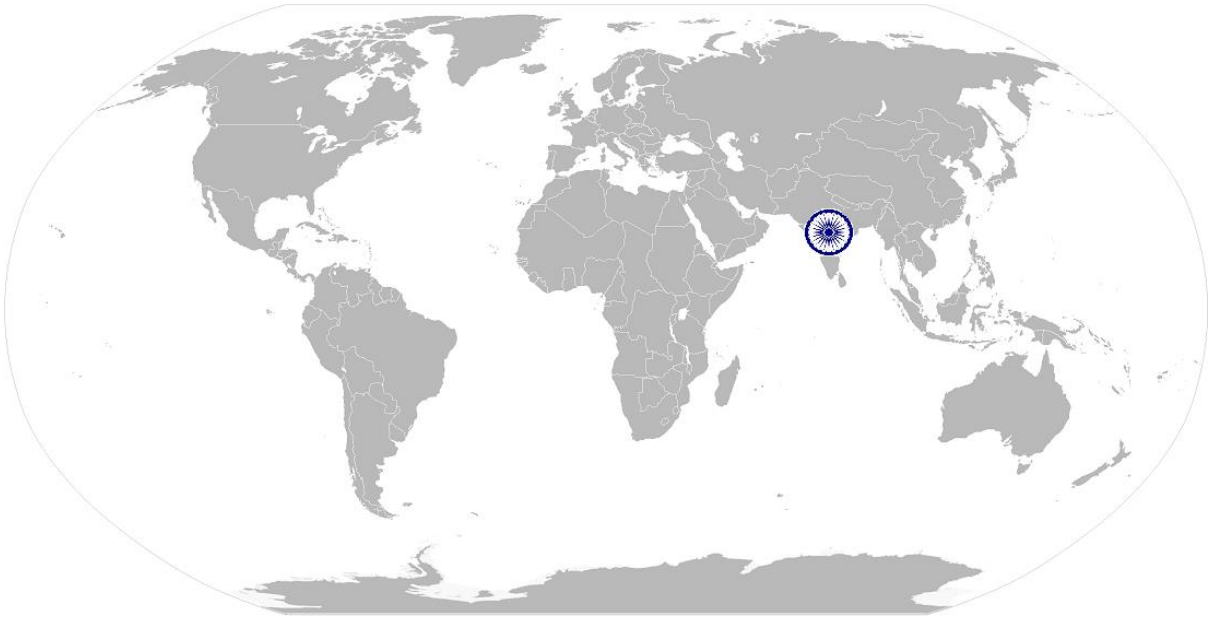
SSC/N9001 Manage your work to meet requirements

	SB5. check that your own work meets customer requirements
	Problem Solving
	You need to know and understand how to: SB6. refer anomalies to the line manager SB7. seek clarification on problems from others
	Analytical Thinking
	You need to know and understand how to: SB8. provide relevant information to others SB9. analyze needs, requirements and dependencies in order to meet your work requirements
	Critical Thinking
	You need to know and understand how to: SB10. apply judgments to different situations
	Attention to Detail
	You need to know and understand how to: SB11. check your work is complete and free from errors SB12. get your work checked by peers
	Team Working
	You need to know and understand how to: SB13. work effectively in a team environment
C. Technical Skills	You need to know and understand how to: SC1. use information technology effectively, to input and/or extract data accurately SC2. identify and refer anomalies in data SC3. store and retrieve information SC4. keep up to date with changes, procedures and practices in your role

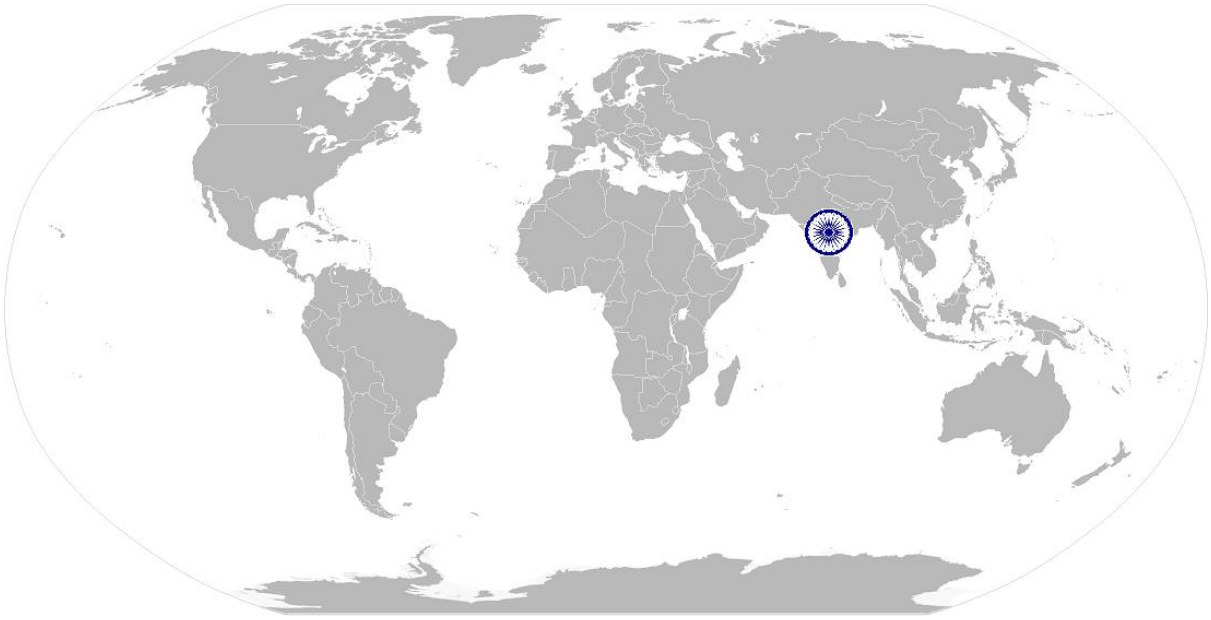
SSC/N9001 **Manage your work to meet requirements**

NOS Version Control

NOS Code	SSC/N9001		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	15/03/2016
Industry Sub-sector	IT Services	Last reviewed on	15/03/2016
		Next review date	15/03/2017



National Occupational Standard



Overview

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

SSC/N9002 **Work effectively with colleagues**

Applicable NOS Unit

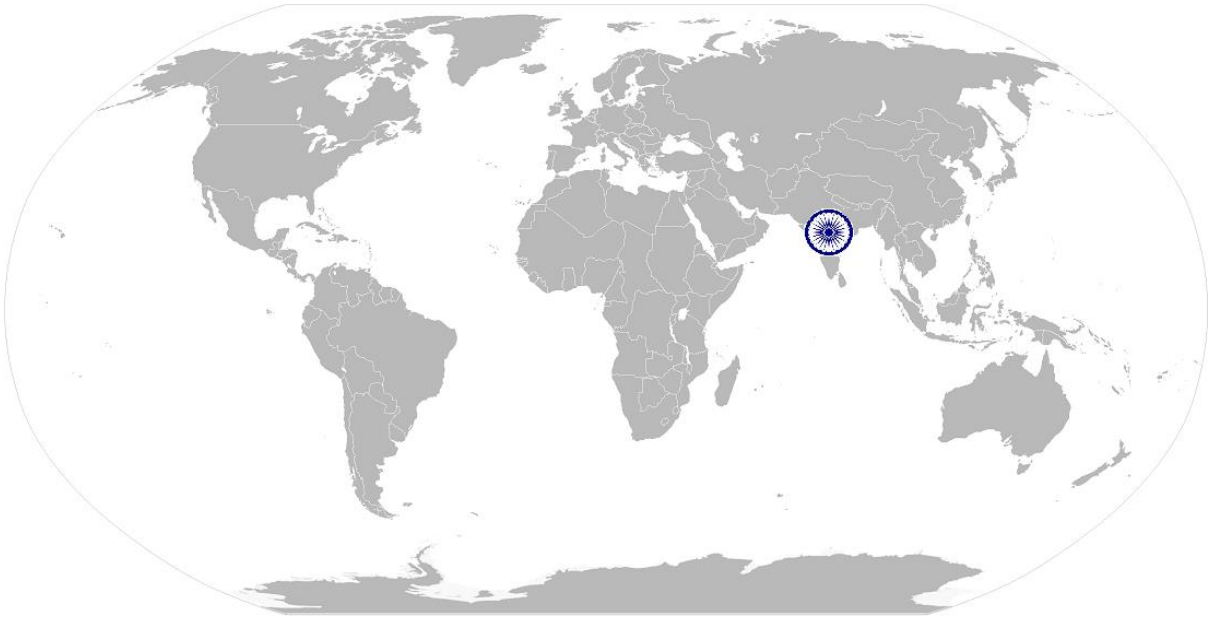
Unit Code	**SSC/N9002**
Unit Title (Task)	**Work effectively with colleagues**
Description	This unit is about working effectively with colleagues, either in your own work group or in other work groups within your organization.
Scope	This unit/task covers the following: **Colleagues**: • line manager • members of your own work group • people in other work groups in your organization **Communicate**: • face-to-face • by telephone • in writing
Performance Criteria (PC) w.r.t. the Scope	
	To be competent, you must be able to: PC1. **communicate** with **colleagues** clearly, concisely and accurately PC2. work with **colleagues** to integrate your work effectively with them 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 organization's policies and procedures for working with **colleagues**
Knowledge and Understanding (K)	
A. Organizational Context (Knowledge of the company/ organization and its processes)	You need to know and understand: KA1. your organization's policies and procedures for working with colleagues and your role and responsibilities in relation to this KA2. the importance of effective communication and establishing good working relationships with colleagues KA3. different methods of communication and the circumstances in which it is appropriate to use these KA4. benefits of developing productive working relationships with colleagues KA5. the importance of creating an environment of trust and mutual respect in an

SSC/N9002 **Work effectively with colleagues**

	environment where you have no authority over those you are working with KA6. where you do not meet your commitments, the implications this will have on individuals and the organization
B. Technical Knowledge	You need to know and understand: KB1. different types of information that colleagues might need and the importance of providing this information when it is required KB2. the importance of understanding problems from your colleague's perspective and how to provide support, where necessary, to resolve these
Skills (S)	
A. Core Skills/ Generic Skills	**Writing Skills**
	You need to know and understand how to: SA1. complete accurate, well written work with attention to detail SA2. communicate effectively with colleagues in writing
	Reading Skills
	You need to know and understand how to: SA3. read instructions, guidelines, procedures, rules and service level agreements
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA4. listen effectively and orally communicate information accurately SA5. ask for clarification and advice from line managers
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. make a decision on a suitable course of action
	Plan and Organize
	You need to know and understand how to: SB2. plan and organize your work to achieve targets and deadlines
	Customer Centricity
	You need to know and understand how to: SB3. check that your own work meets customer requirements SB4. deliver consistent and reliable service to customers
	Problem Solving
	You need to know and understand how to: SB5. apply problem solving approaches in different situations
	Critical Thinking
	You need to know and understand how to: SB6. apply balanced judgments to different situations
	Attention to Detail
	You need to know and understand how to: SB7. check your work is complete and free from errors

SSC/N9002 **Work effectively with colleagues**

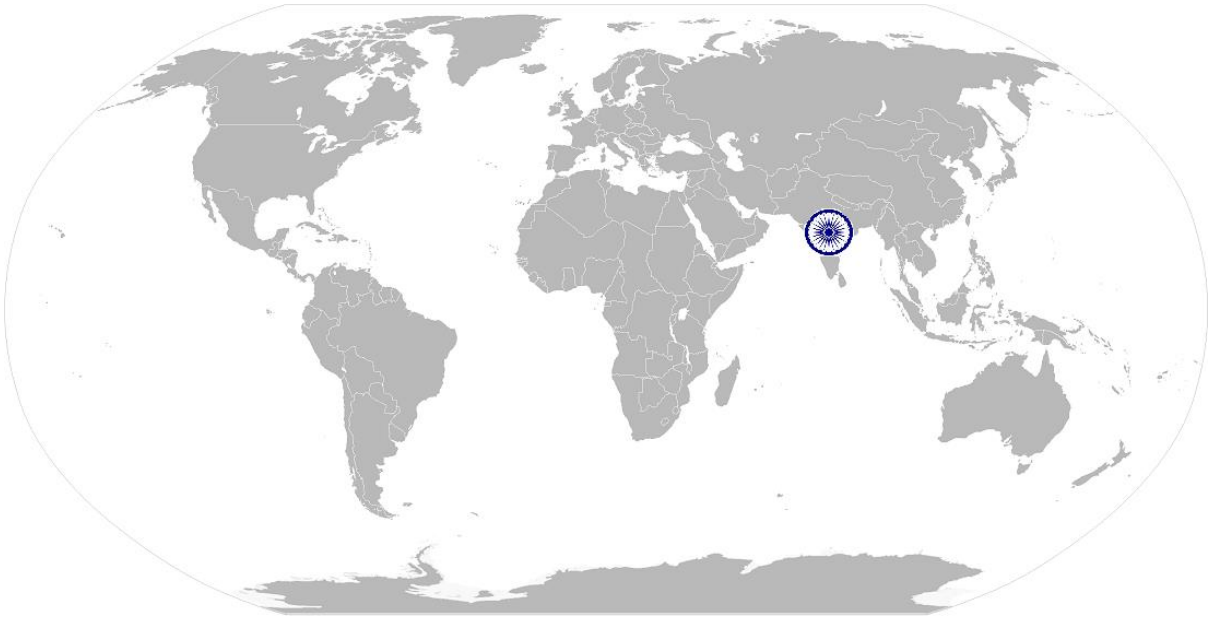
	SB8. get your work checked by peers
	Team Working
	You need to know and understand how to: SB9. work effectively in a team environment SB10. work effectively with colleagues and other teams SB11. treat other cultures with respect
C. Technical Skills	You need to know and understand how to: SC1. identify and refer anomalies SC2. help reach agreements with colleagues SC3. keep up to date with changes, procedures and practices in your role



SSC/N9002 **Work effectively with colleagues**

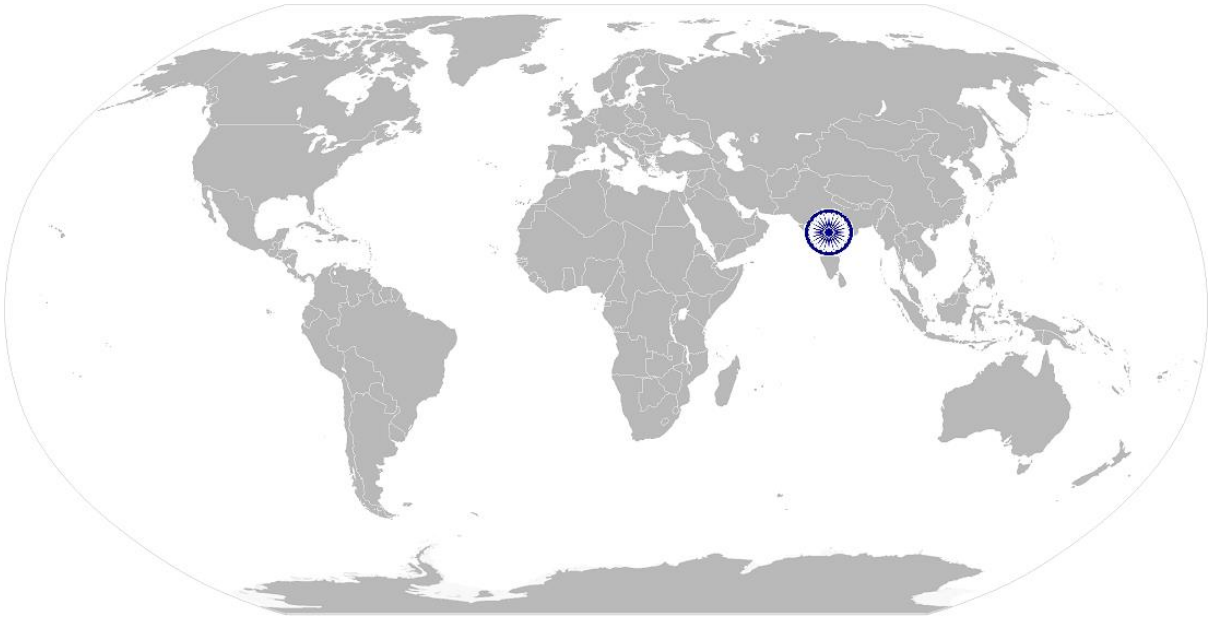
NOS Version Control

NOS Code	SSC/N9002		
Credits(NVEQF/NVQF/NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	15/03/2016
Industry Sub-sector	IT Services	Last reviewed on	15/03/2016
		Next review date	15/03/2017



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

National Occupational Standard



Overview

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

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

Applicable NOS Unit

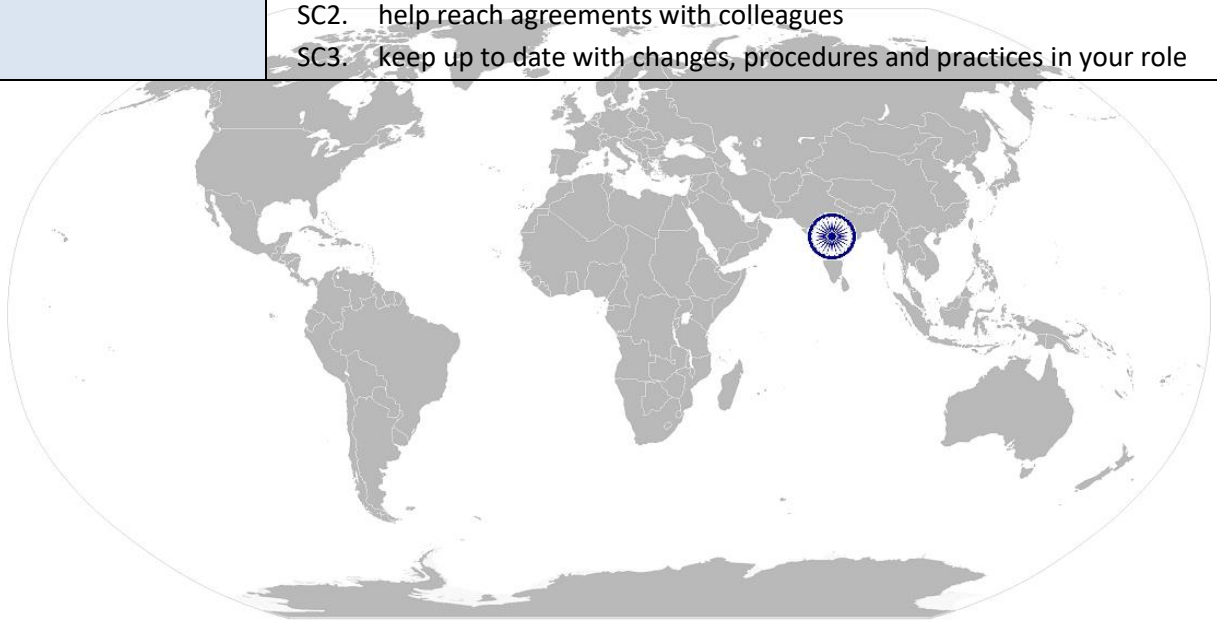
Unit Code	SSC/N9003
Unit Title (Task)	**Maintain a healthy, safe and secure working environment**
Description	This unit is about monitoring your working environment and making sure it meets requirements for health, safety and security.
Scope	This unit/task covers the following: **Emergency procedures**: • illness • accidents • fires • other reasons to evacuate the premises • breaches of security
Performance Criteria (PC) w.r.t. the Scope	
	To be competent, you must be able to: PC1. comply with your organization's 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 organization's **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 (K)	
A. Organizational Context (Knowledge of the company/ organization and its processes)	You need to know and understand: KA1. legislative requirements and organization's procedures for health, safety and security and your role and responsibilities in relation to this KA2. what is meant by a hazard, including the different types of health and safety hazards that can be found in the workplace KA3. how and when to report hazards KA4. limits of your responsibility for dealing with hazards KA5. your organization's **emergency procedures** for different emergency situations and the importance of following these

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

	KA6. the importance of maintaining high standards of health, safety and security KA7. implications that any non-compliance with health, safety and security may have on individuals and the organization
B. Technical Knowledge	You need to know and understand: KB1. different types of breaches in health, safety and security and how and when to report these KB2. evacuation procedures for workers and visitors KB3. how to summon medical assistance and the emergency services, where necessary KB4. how to use the health, safety and accident reporting procedures and the importance of these KB5. government agencies in the areas of safety, health and security and their norms and services
Skills (S)	
A. Core Skills/ Generic Skills	**Writing Skills**
	You need to know and understand how to: SA1. complete accurate, well written work with attention to detail
	Reading Skills
	You need to know and understand how to: SA2. read instructions, guidelines, procedures, rules and service level agreements
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA3. listen effectively and orally communicate information accurately
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. make a decision on a suitable course of action
	Plan and Organize
	You need to know and understand how to: SB2. plan and organize your work to meet health, safety and security requirements
	Customer Centricity
	You need to know and understand how to: SB3. build and maintain positive and effective relationships with colleagues and customers
	Problem Solving
	You need to know and understand how to: SB4. apply problem solving approaches in different situations
	Analytical Thinking
	You need to know and understand how to: SB5. analyze data and activities

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

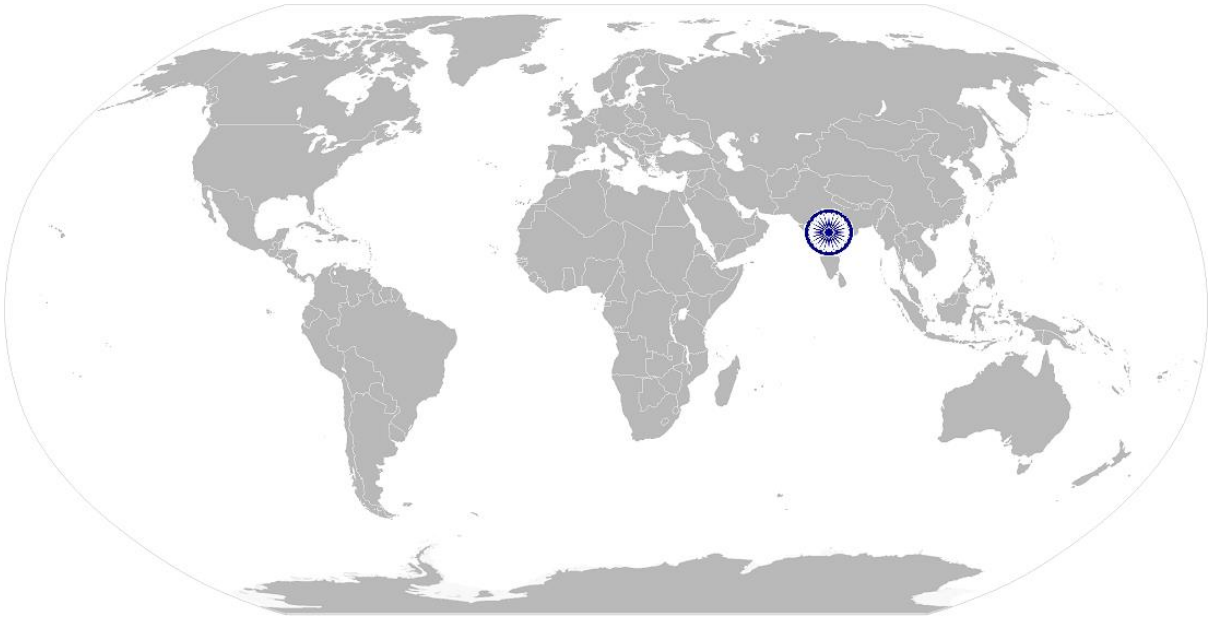
	Critical Thinking
	You need to know and understand how to: SB6. apply balanced judgments to different situations
	Attention to Detail
	You need to know and understand how to: SB7. check your work is complete and free from errors SB8. get your work checked by peers
	Team Working
	You need to know and understand how to: SB9. work effectively in a team environment
C. Technical Skills	You need to know and understand how to: SC1. identify and refer anomalies SC2. help reach agreements with colleagues SC3. keep up to date with changes, procedures and practices in your role



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

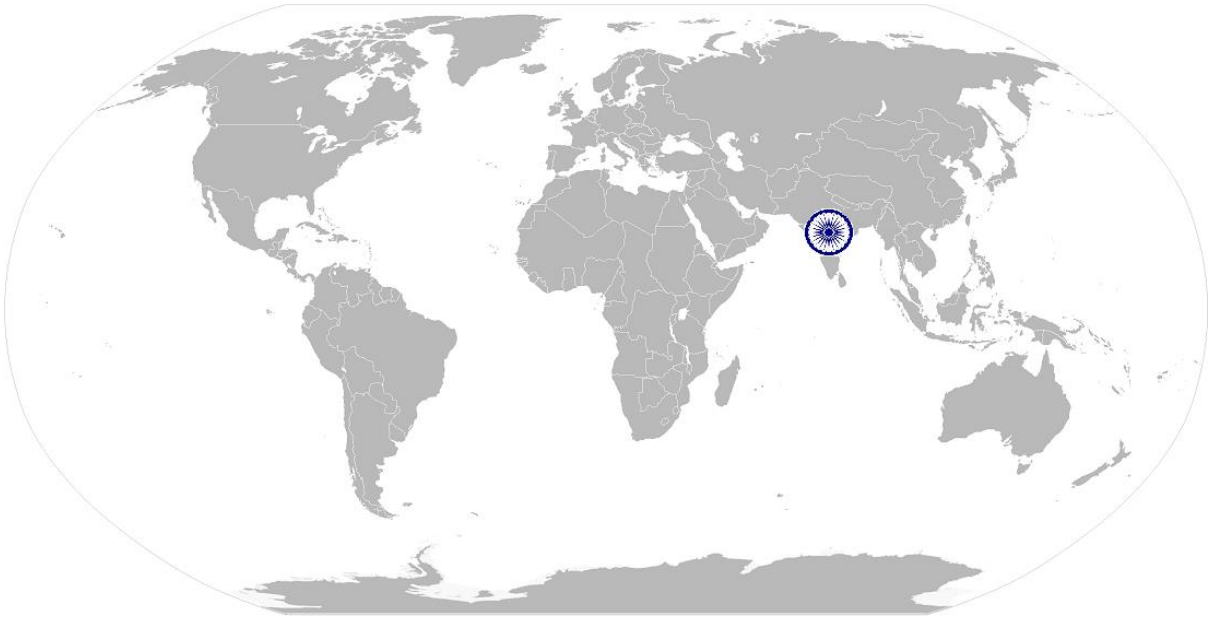
NOS Version Control

NOS Code	SSC/N9003		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	15/03/2016
Industry Sub-sector	IT Services	Last reviewed on	15/03/2016
		Next review date	15/03/2017



SSC/N9004 **Provide data/information in standard formats**

National Occupational Standard



Overview

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

Applicable NOS Unit

SSC/N9004 Provide data/information in standard formats

Unit Code	**SSC/N9004**
Unit Title (Task)	**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 • qualitative **Sources**: • within your organization • outside your organization **Formats**: • paper-based • electronic
Performance Criteria (PC) w.r.t. the Scope	
	To be competent, you 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 agreed **formats** PC7. check the accuracy of your work, involving colleagues where required PC8. report any unresolved anomalies in the **data/information** to **appropriate people**

SSC/N9004	Provide data/information in standard formats
	PC9. provide complete, accurate and up-to-date data/information to the appropriate **people** in the required **formats** on time
Knowledge and Understanding (K)	
A. Organizational Context (Knowledge of the company/ organization and its processes)	You need to know and understand: KA1. your organization's procedures and guidelines for providing data/information in standard formats and your role and responsibilities in relation to this KA2. the knowledge management culture of your organization KA3. your organization's policies and procedures for recording and sharing information and the importance of complying with these KA4. the importance of validating data/information before use and how to do this KA5. procedures for updating data in appropriate formats and with proper validation KA6. the purpose of the CRM database KA7. how to use the CRM database to record and extract information KA8. the importance of having your data/information reviewed by others KA9. the scope of any data/information requirements including the level of detail required KA10. the importance of keeping within the scope of work and adhering to timescales
B. Technical Knowledge	You need to know and understand: KB1. data/information you may need to provide including the sources and how to do this KB2. templates and formats used for data/information including their purpose and how to use these KB3. different techniques used to obtain data/information and how to apply KB4. these KB5. how to carry out rule-based analysis on the data/information KB6. typical anomalies that may occur in data/information KB7. who to go to in the event of inaccurate data/information and how to report this
Skills (S)	
A. Core Skills/ Generic Skills	**Writing Skills**
	You need to know and understand how to: SA1. complete accurate, well written work with attention to detail
	Reading Skills
	You need to know and understand how to: SA2. read instructions, guidelines, procedures, rules and service level agreements
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to:

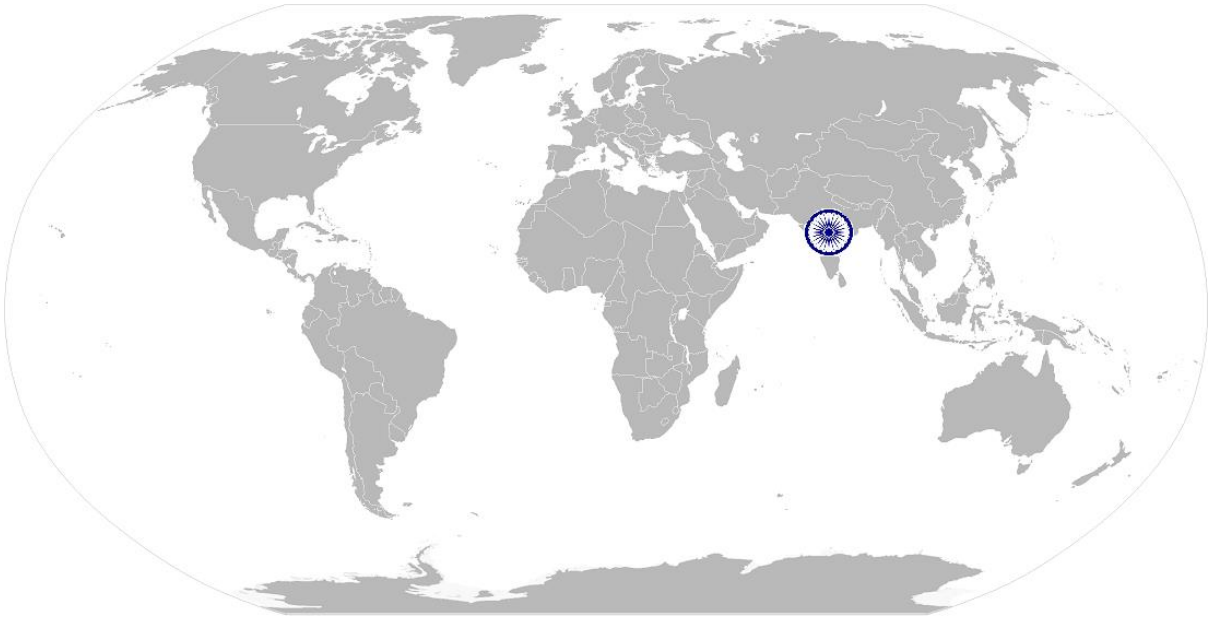
SSC/N9004 Provide data/information in standard formats

	SA3. listen effectively and orally communicate information accurately
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. follow rule-based decision-making processes SB2. make a decision on a suitable course of action
	Plan and Organize
	You need to know and understand how to: SB3. plan and organize your work to achieve targets and deadlines
	Customer Centricity
	You need to know and understand how to: SB4. check that your own work meets customer requirements SB5. meet and exceed customer expectations
	Problem Solving
	You need to know and understand how to: SB6. apply problem solving approaches in different situations
	Analytical Thinking
	You need to know and understand how to: SB7. configure data and disseminate relevant information to others
	Critical Thinking
	You need to know and understand how to: SB8. apply balanced judgments to different situations
	Attention to Detail
	You need to know and understand how to: SB9. check your work is complete and free from errors SB10. get your work checked by peers
	Team Working
	You need to know and understand how to: SB11. work effectively in a team environment
C. Technical Skills	You need to know and understand how to: SC1. use information technology effectively, to input and/or extract data accurately SC2. validate and update data SC3. identify and refer anomalies in data SC4. store and retrieve information SC5. share information using standard formats and templates SC6. keep up to date with changes, procedures and practices in your role

SSC/N9004 **Provide data/information in standard formats**

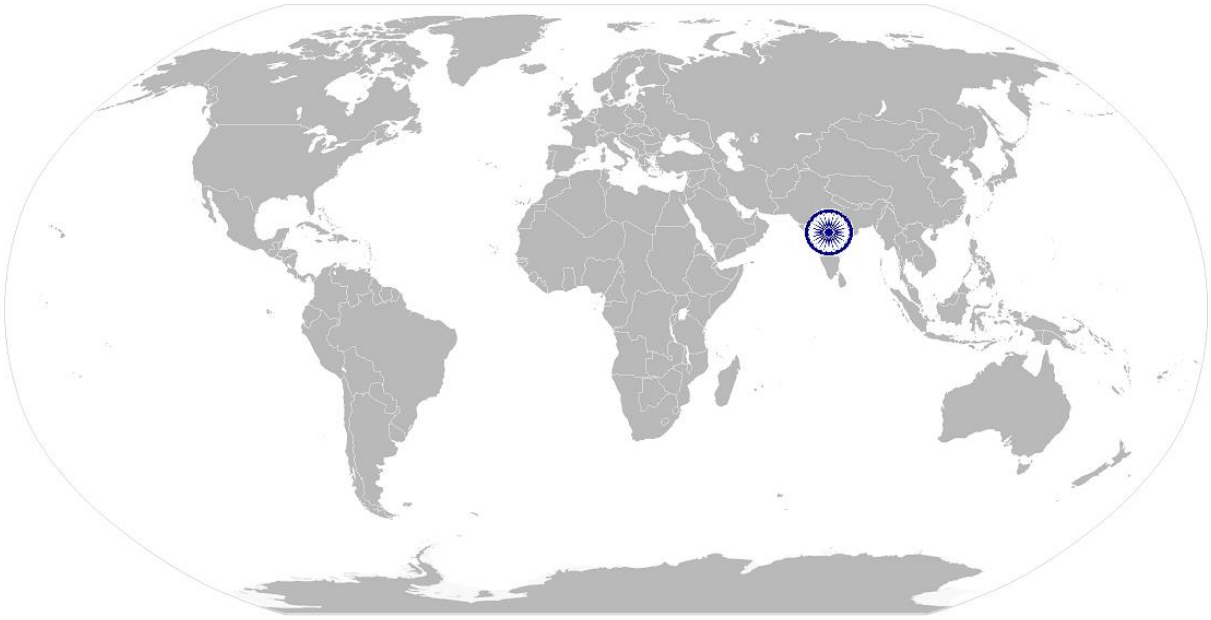
NOS Version Control

NOS Code	SSC/N9004		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	15/03/2016
Industry Sub-sector	IT Services	Last reviewed on	15/03/2016
		Next review date	15/03/2017



SSC/N9005 **Develop your knowledge, skills and competence**

National Occupational Standard



Overview

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.

SSC/N9005 Develop your knowledge, skills and competence

Applicable NOS Unit

Unit Code	**SSC/N9005**
Unit Title (Task)	**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 **Different methods** • training need analysis • skills need analysis • performance appraisals
Performance Criteria (PC) w.r.t. the Scope	
	To be competent, you 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

SSC/N9005 **Develop your knowledge, skills and competence**

	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 (K)	
A. Organizational Context (Knowledge of the company/ organization and its processes)	You need to know and understand: KA1. your organization's procedures and guidelines for developing your knowledge, skills and competence and your role and responsibilities in relation to this KA2. the importance of developing your knowledge, skills and competence to you and your organization KA3. **different methods** used by your organization to review skills and knowledge KA4. how to review your knowledge and skills against your job role using different methods and analysis KA5. different types of learning and development activities available for your job role and how to access these KA6. 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 KA7. different types of support available to help you plan and undertake learning and development activities and how to access these KA8. why it is important to maintain records of your learning and development KA9. methods of obtaining and accepting feedback from appropriate people on your knowledge skills and competence KA10. how to use feedback to develop in your job role
B. Technical Knowledge	You need to know and understand: KB1. the knowledge and skills required in your job role KB2. your current learning and development needs in relation to your job role KB3. different types of learning styles and methods including those that help you learn best KB4. the importance of taking responsibility for your own learning and development KB5. to the importance of learning and practicing new concepts, theory and how to apply these in the work environment or on samples. KB6. how to explore sample problems and apply solutions
Skills (S)	
A. Core Skills/	**Writing Skills** You need to know and understand how to:

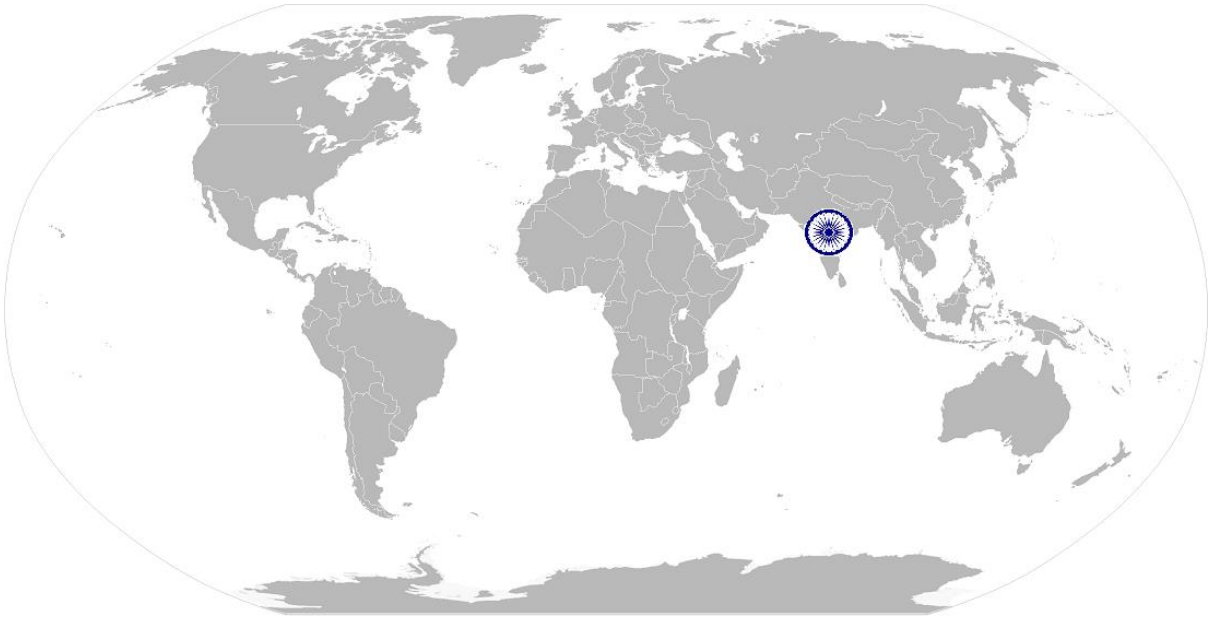
SSC/N9005 **Develop your knowledge, skills and competence**

Generic Skills	SA1. communicate with colleagues in writing
	Reading Skills
	You need to know and understand how to: SA2. read instructions, guidelines and procedures
	Oral Communication (Listening and Speaking skills)
	You need to know and understand how to: SA3. ask for clarification and advice from line managers
B. Professional Skills	**Decision Making**
	You need to know and understand how to: SB1. make a decision on a suitable course of action
	Plan and Organize
	You need to know and understand how to: SB2. plan and organize your work to achieve targets and deadlines
	Customer Centricity
	You need to know and understand how to: SB3. check that your own work meets customer requirements
	Problem Solving
	You need to know and understand how to: SB4. refer anomalies to the line manager
	Analytical Thinking
	You need to know and understand how to: SB5. analyze data and activities
	Critical Thinking
	You need to know and understand how to: SB6. apply balanced judgments to different situations
	Attention to Detail
	You need to know and understand how to: SB7. check your work is complete and free from errors SB8. get your work checked by peers
	Team Working
	You need to know and understand how to: SB9. work effectively in a team environment
C. Technical Skills	You need to know and understand how to: SC1. use information technology effectively SC2. agree objectives and work requirements SC3. keep up to date with changes, procedures and practices in your role

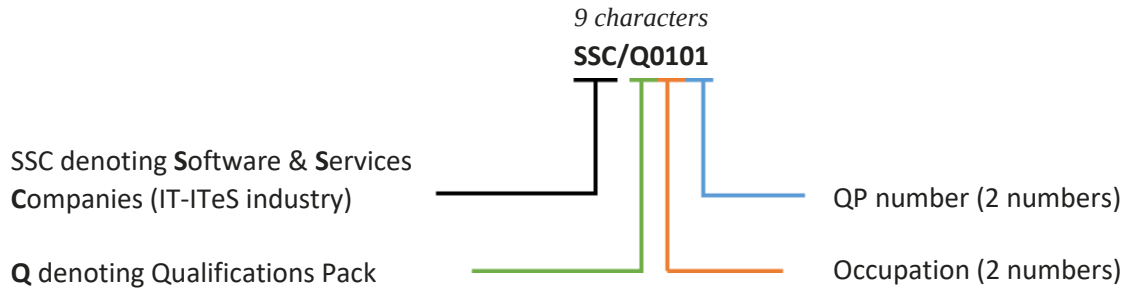
SSC/N9005 **Develop your knowledge, skills and competence**

NOS Version Control

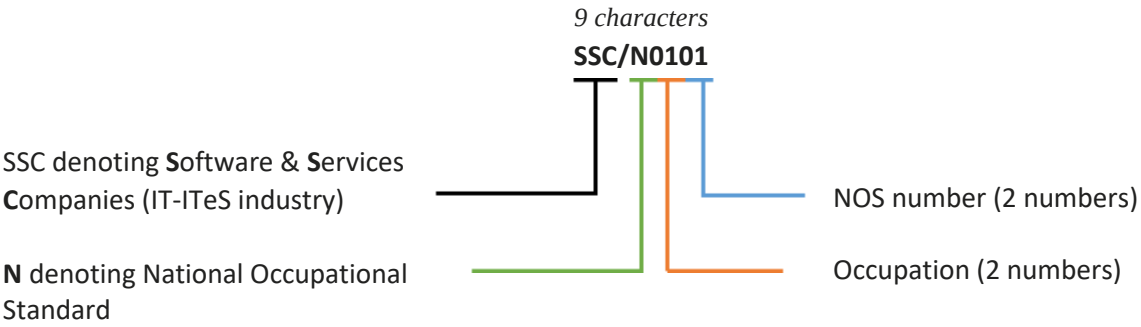
NOS Code	SSC/N9005		
Credits (NSQF)	TBD	Version number	1.0
Industry	IT-ITeS	Drafted on	15/03/2016
Industry Sub-sector	IT Services	Last reviewed on	15/03/2016
		Next review date	15/03/2017



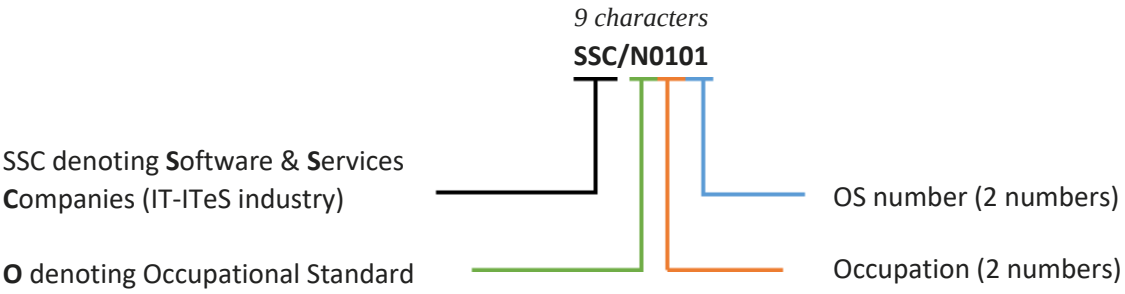
Qualifications Pack



National Occupational Standard



Occupational Standard



It is important to note that an OS unit can be denoted with either an '**O**' or an '**N**'.

- If an OS unit denotes 'O', it is an OS unit that is an international standard. An example of OS unit denoting 'O' is SSC/**O**0101.
- If an OS unit denotes '**N**', it is an OS unit that is a national standard and is applicable only for the Indian IT-ITeS industry. An example of OS unit denoting '**N**' is SSC/N0101

Nomenclature for QP and NOS Units

The following acronyms/codes have been used in the nomenclature above:

Sub-Sector	Range of Occupation numbers
IT Service (ITS)	01-20
Business Process Management (BPM)	21-40
Engg. and R&D (ERD)	41-60
Software Products (SPD)	61-80

Sequence	Description	Example
Three letters	Industry name (Software & Service Companies)	SSC
Slash	/	/
Next letter	Whether **Q**P or **N**OS	N
Next two numbers	Occupation Code	01
Next two numbers	OS number	01

Criteria for Assessment of Trainees

Job Role	Forensic Specialist
Qualification Pack	SSC/Q0922
Sector Skill Council	IT-ITeS

Guidelines for Assessment:

1. Criteria for assessment for each Qualification Pack (QP) will be created by the Sector Skill Council (SSC). Each performance criteria (PC) will be assigned Theory and Skill/Practical marks proportional to its importance in NOS.
2. The assessment will be conducted online through assessment providers authorized 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.

		Mark Allocation			
Assessment Outcomes	**Assessment Criteria for Outcomes**	**Total Marks**	**Out of**	**Theory**	**Skills Practical**
1. SSC/N0929 (Identify, preserve and seize digital/electronics devices or records for investigation of possible breach or crime)	PC1. ensure that necessary authorisations and resources are in place to conduct a forensics evidence seizure for an investigation	**100**	3	1	2
	PC2. ensure that the scene is physically secured to prevent unauthorized access and alteration or damage of the evidence as per containment policies and situational considerations		4	2	2
	PC3. survey a physical area and identify potential sources of data that could be evidence		4	1	3
	PC4. identify other sources of data and the owner of the same that can be accessed		3	1	2
	PC5. identify and obtain materials related to digital communications which are relevant to the investigation		3	1	2
	PC6. ensure identified device or component is up and running however is being disconnected from any network		3	1	2

Criteria for Assessment of Trainees

	PC7. check for and terminate any destructive software running on any device while seeking to save as much information as possible		4	1	3
	PC8. estimate the relative likely value of each potential data source for the investigation		4	1	3
	PC9. identify whether data in the device or record is volatile or non-volatile so that both types of data can be adequately preserved		4	1	3
	PC10. create a plan that prioritizes the sources, establishing the order in which the computing devices or records can be acquired		5	2	3
	PC11. use forensic tools to collect volatile data		5	2	3
	PC12. duplicate non-volatile data sources to collect their data, securing the original non-volatile data sources		5	2	3
	PC13. verify and preserve the integrity of the data source device or record in accordance with investigation procedures		5	1	4
	PC14. record current state, condition and configuration of digital devices and media and potentially relevant information at the time of seizure		6	2	4
	PC15. handle digital devices and media consistent with preserving other potential evidence sources including fingerprints or DNA		3	1	2
	PC16. document any activity on the computer, components, or devices by taking photographs or recording any information that may be relevant		4	1	3
	PC17. maintain a detailed log of every step that was taken to collect the data, including information about each tool used in the process and handlers		4	1	3

Criteria for Assessment of Trainees

	PC18. photograph and label the components of the device making specific reference to ancillary leads and connections to the device		4	1	3
	PC19. appropriately package, seal and label the device in accordance with current diligence procedures		3	1	2
	PC20. check packaging of forensic items in line with forensic procedures, and identify, record and address any packaging problems		4	1	3
	PC21. carefully document each stage of the seizure and investigation		3	1	2
	PC22. ensure chain of custody is followed for all digital media acquired in accordance with the rules of evidence		3	1	2
	PC23. identify any risks to safety linked to working with forensic items in line with health and safety procedures		3	1	2
	PC24. take the necessary actions to minimise any risks linked to working with forensic items		4	1	3
	PC25. transport and store forensic items to relevant authorities in line with investigative procedures, and in a way that avoids risk to potential evidence, including loss, breakage, contamination, cross-contamination, degradation, etc.		4	1	3
	PC26. record details of the storage, handling, transfer and packaging of forensic items in line with organisational procedures		3	1	2
		Total	**100**	**31**	**69**
2. SSC/N0930 (Extract relevant data or information from digital forensic evidences)	PC1. obtain items relevant to forensic examinations in line with investigative procedures from authorised channels	**100**	3	1	2
	PC2. check forensic items against records and identify and address any inaccuracies		4	1	3

Criteria for Assessment of Trainees

PC3. identify and obtain necessary resources that could be required for extracting relevant data or information from the evidences	3	1	2
PC4. create an image or copy of the original storage device using clean storage media to have a backup	5	2	3
PC5. install write blocking software to prevent any change to the data on the device or media	5	2	3
PC6. identify data that is required to be extracted and most likely sources	3	1	2
PC7. select the best method and tools for extraction as per the make and model of device	2	1	1
PC8. locate the required files manually or using forensic tools	3	1	2
PC9. display the contents of slack space with hex editors or special slack recovery tools	3	1	2
PC10. hunt for files and information that have been hidden, deleted or lost	3	1	2
PC11. identify the type of data stored in many files by looking at their file headers or simple histogram	3	1	2
PC12. identify presence of encrypted data or the use of steganography and the feasibility of decryption or extracting embedded data	3	1	2
PC13. identify the encryption method by examining the file header, identifying encryption programs installed on the system, or finding encryption keys	4	1	3
PC14. extract the embedded data by finding the stego key, or by using brute force and cryptographic attacks to determine a password	5	1	4
PC15. crack, disable or bypass passwords placed on individual files, as well as OS passwords using various utilities and	4	1	3

techniques				
PC16. find, recover and copy data from disks that may have been hidden, encrypted or damaged, etc.	4	1	3
PC17. uncompress files and read disk images	3	1	2
PC18. extract data and metadata from files using forensic toolkits	4	1	3
PC19. identify malicious activity against OSs using security applications, such as file integrity checkers and host IDSs, etc.	4	2	2
PC20. perform string searches and pattern matching using searching tools that use Boolean, fuzzy logic, synonyms and concepts, stemming, and other search methods	5	1	4
PC21. assess and extract network traffic data with the goal of determining what happened and how the organization's systems and networks have been affected	4	1	3
PC22. obtain relevant information from ISP and cloud service provider after taking due authorisation from Law Enforcement Authority/Agency	3	1	2
PC23. reveal (unlock) digital images that have been altered to mask the identity of a place or person	4	1	3
PC24. submit the device or original media for physical evidence examination after removing the data	3	0	3
PC25. when equipment is damaged, dismantle and rebuild the system in order to recover lost data	4	1	3
PC26. carefully document the process followed in extraction as well as the data retrieved	3	1	2
PC27. identify and minimise any risks to safety linked to working with forensic items in line with health and safety procedures	3	1	2

	PC28. take measures to ensure preservation of physical evidence like finger prints, DNA etc. while handling the evidence		3	1	2
		Total	**100**	**30**	**70**
3. SSC/N0931 (Analyze information or data extracted from digital forensic evidences)	PC1. identify and obtain necessary resources that could be required for examining and analysing of forensic evidences	**100**	3	1	2
	PC2. perform analysis of the extracted data using various forensic tools		5	2	3
	PC3. review the time and date stamps contained in the file system metadata to link files of interest to the timeframes relevant to the investigation		3	1	2
	PC4. review system and application logs for relevant information		3	1	2
	PC5. correlate file headers to the corresponding file extensions to identify any mismatches		3	1	2
	PC6. perform data hiding analysis for detecting and recovering data and may indicate knowledge, ownership, or intent		5	1	4
	PC7. analyse programs and files in various ways to provide insight into the capability of the system and the knowledge of the user		5	1	4
	PC8. analyse file metadata typically through the application that created it to provide insight into detailed information like authorship, time last edited, number of times edited, and print or saved location, etc.		5	1	4
	PC9. determine ownership and knowledgeable possession of the questioned data using various methods		4	1	3

Criteria for Assessment of Trainees

	PC10. analyze network traffic data with the goal of determining what has happened and how the organization's systems and networks have been affected	5	1	4
	PC11. analyse mobile phone records to trace devices to a particular location (or to rule them out)	4	2	2
	PC12. follow electronic data trails to uncover links between individuals or groups	4	1	3
	PC13. piece together strings of interactions that provide a picture of activity using evidence collected from other sources than electronic devices	5	2	3
	PC14. identify additional systems/networks compromised by cyber attacks	3	1	2
	PC15. identify the most important characteristics of the activity and the negative impact it has caused or may cause the organization	4	2	2
	PC16. perform computer network defense (CND) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation	6	2	4
	PC17. perform various types of forensics analysis as per the requirement of media type, data or contraints	6	2	4
	PC18. perform virus scanning on digital media	4	1	3
	PC19. fuse computer network attack analyses with criminal and counterintelligence investigations and operations	4	1	3
	PC20. identify elements of proof of the crime	3	1	2
	PC21. identify outside attackers accessing the system from the internet or insider attackers, that is, authorized users attempting to gain and misuse non-	3	1	2

	authorized privileges				
	PC22. follow investigation procedure in order to determine the identity of attacker		3	1	2
	PC23. take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations		3	1	2
	PC24. carefully document each stage of the investigation		3	1	2
	PC25. identify risks to safety linked to working with forensic items and take the necessary actions to minimise the risks		4	1	3
		Total	**100**	**31**	**69**
4. SSC/N0932 (Report and present the results of a forensic investigation)	PC1. identify and obtain necessary resources that could be required for reporting and presenting forensic investigation, its results and evidences	**100**	7	2	5
	PC2. ensure all relevant information is collated and captured in the report accurately and clearly		6	2	4
	PC3. list and organise for supporting materials that are included with the report, such as printouts of particular items of evidence, digital copies of evidence, chain of custody documentation, photos, emails (showing email headers, the path and timing emails took to get from source to destination), etc.		9	3	6
	PC4. create a brief summary of the results of the examinations performed on the items submitted for analysis		9	3	6
	PC5. provide comprehensive details of findings in the report		9	3	6
	PC6. create a glossary with the report to assist the reader using an accepted source for the definition of the terms and include appropriate references		6	2	4
	PC7. ensure that the evidence remains		5	1	4

	pristine and unaltered while presenting				
	PC8. present and explain track record of information exchange, and the "hash!value", also referred to as a checksum, as a mark of authenticity		6	2	4
	PC9. carefully document each stage of your investigation		7	2	5
	PC10. work within the level of authority and expertise taking actions necessary should these be exceeded		6	2	4
	PC11. differentiate between fact and opinion and express opinions within your area of expertise while writing the report		5	1	4
	PC12. identify any risks to safety linked to working with forensic items in line with health and safety procedures		5	2	3
	PC13. take the necessary actions to minimise any risks linked to working with forensic items		6	2	4
	PC14. take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations		7	2	5
	PC15. take appropriate action to ensure confidentiality and integrity of report and related documents		7	2	5
		Total	**100**	**31**	**69**
4. SSC/N9001 (Manage your work to meet requirements)	PC1. establish and agree your work requirements with appropriate people	**100**	7	0	7
	PC2. keep your immediate work area clean and tidy		12	6	6
	PC3. utilize your time effectively		12	6	6
	PC4. use resources correctly and efficiently		19	6	13
	PC5. treat confidential information correctly		7	1	6
	PC6. work in line with your organization's policies and procedures		12	0	12

	PC7. work within the limits of your job role		6	0	6
	PC8. obtain guidance from appropriate people, where necessary		6	0	6
	PC9. ensure your work meets the agreed requirements		19	6	13
		Total	**100**	**25**	**75**
5. SSC/N9002 (Work effectively with colleagues)	PC1. communicate with colleagues clearly, concisely and accurately	**100**	20	0	20
	PC2. work with colleagues to integrate your work effectively with theirs		10	0	10
	PC3. pass on essential information to colleagues in line with organizational requirements		10	10	0
	PC4. work in ways that show respect for colleagues		20	0	20
	PC5. carry out commitments you have made to colleagues		10	0	10
	PC6. let colleagues know in good time if you cannot carry out your commitments, explaining the reasons		10	10	0
	PC7. identify any problems you have working with colleagues and take the initiative to solve these problems		10	0	10
	PC8. follow the organization's policies and procedures for working with colleagues		10	0	10
		Total	**100**	**20**	**80**
6. SSC/N9003 (Maintain a healthy, safe and secure working environment)	PC1. comply with your organization's current health, safety and security policies and procedures	**100**	20	10	10
	PC2. report any identified breaches in health, safety, and security policies and procedures to the designated person		10	0	10
	PC3. identify and correct any hazards that you can deal with safely, competently and within the limits of your authority		20	10	10
	PC4. report any hazards that you are not competent to deal with to the relevant		10	0	10

	person in line with organizational procedures and warn other people who may be affected				
	PC5. follow your organization's emergency procedures promptly, calmly, and efficiently		20	10	10
	PC6. identify and recommend opportunities for improving health, safety, and security to the designated person		10	0	10
	PC7. complete any health and safety records legibly and accurately		10	0	10
		Total	**100**	**30**	**70**
7. SSC/N9004 (Provide data/information in standard formats)	PC1. establish and agree with appropriate people the data/information you need to provide, the formats in which you need to provide it, and when you need to provide it	**100**	13	13	0
	PC2. obtain the data/information from reliable sources		13	0	13
	PC3. check that the data/information is accurate, complete and up-to-date		12	6	6
	PC4. obtain advice or guidance from appropriate people where there are problems with the data/information		6	0	6
	PC5. carry out rule-based analysis of the data/information, if required		25	0	25
	PC6. insert the data/information into the agreed formats		13	0	13
	PC7. check the accuracy of your work, involving colleagues where required		6	0	6
	PC8. report any unresolved anomalies in the data/information to appropriate people		6	6	0
	PC9. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time		6	0	6
		Total	**100**	**25**	**75**

Criteria for Assessment of Trainees

8. SSC/N9005 (Develop your knowledge, skills and competence)	PC1. obtain advice and guidance from appropriate people to develop your knowledge, skills and competence	**100**	10	0	10
	PC2. identify accurately the knowledge and skills you need for your job role		10	0	10
	PC3. identify accurately your current level of knowledge, skills and competence and any learning and development needs		20	10	10
	PC4. agree with appropriate people a plan of learning and development activities to address your learning needs		10	0	10
	PC5. undertake learning and development activities in line with your plan		20	10	10
	PC6. apply your new knowledge and skills in the workplace, under supervision		10	0	10
	PC7. obtain feedback from appropriate people on your knowledge and skills and how effectively you apply them		10	0	10
	PC8. review your knowledge, skills and competence regularly and take appropriate action		10	0	10
		Total	**100**	**20**	**80**