Qualification Pack

Analyst Application Security

QP Code: SSC/Q0903

Version: 4.0

NSQF Level: 5

IT-ITeS SSC NASSCOM || NASSCOM Plot No - 7, 8, 9 & 10, 3rd Floor, Sector 126
Noida Uttar Pradesh - 201303 || email:sscstandards@nasscom.in

Contents

SSC/Q0903: Analyst Application Security

Brief Job Description

The job involves managing application security hardening and vulnerability assessments, accessing APIs to ensure secure integration, and overseeing the security of deployed applications and solutions. The role focuses on monitoring for potential breaches and compromises, implementing security measures, and maintaining robust defenses against evolving cybersecurity threats.

Personal Attributes

This job may require the individual to work independently and take decisions for his/her own area of work. The individual should be result oriented and have a high attention for detail. The individual should also be able to demonstrate communication skills, logical thinking along with willingness to undertake desk-based job with long hours.

Applicable National Occupational Standards (NOS)

Compulsory NOS:

1. SSC/N0958: Access API and application for security
2. SSC/N0959: Manage application security, hardening and vulnerability
3. SSC/N0960: Oversee the Cloud security of deployed applications and solutions to detect potential breaches and compromises
4. DGT/VSQ/N0102: Employability Skills (60 Hours)

Qualification Pack (QP) Parameters

Sector	IT-ITeS
Sub-Sector	Future Skills
Occupation	Information and Cyber Security
Country	India
NSQF Level	5
Credits	17
Aligned to NCO/ISCO/ISIC Code	NCO-2015/NIL

Minimum Educational Qualification & Experience	Completed 2nd year of UG (UG Diploma) (of 3-year/ 4-year UG) with NA of experience OR Completed 3 year diploma after 10th with 1.5 years of experience in relevant field OR Previous relevant Qualification of NSQF Level (4) with 3 Years of experience in relevant field
Minimum Level of Education for Training in School	Not Applicable
Pre-Requisite License or Training	NA
Minimum Job Entry Age	18 Years
Last Reviewed On	NA
Next Review Date	18/02/2028
NSQC Approval Date	18/02/2025
Version	4.0
Reference code on NQR	QG-05-IT-03637-2025-V2-NASSCOM
NQR Version	4.0

SSC/N0958: Access API and application for security

Description

The OS unit is about accessing APIs and applications securely while ensuring compliance with security protocols to prevent unauthorized access and data breaches.

Scope

The scope covers the following :

- Application Security Assessment and Data Validation
- Application Security Assessment and Vulnerability Management
- Comprehensive Application Security and Penetration Testing

Elements and Performance Criteria

Application Security Assessment and Data Validation

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

PC1. review and collect initial information about the application from available data

PC2. assess the importance of information by considering multiple influencing factors like nature of the data, source of the data, size of the data and others

PC3. identify the application type/category by considering various factors like Programming languages, React, Angular, Spring frameworks and others

PC4. demonstrate the ability to assess and implement API authentication, authorization, rate limiting, and data validation to ensure secure and efficient API operations

PC5. conduct targeted assessments to validate and ensure the security of API operations, addressing vulnerabilities related to authentication, authorization, and data integrity

PC6. implement API gateway security measures, including rate limiting and authentication, to ensure secure and efficient API operations

PC7. assess applications to identify and address misconfigurations and supply chain vulnerabilities, ensuring alignment with security standards and best practices

PC8. collect data on application patching and its interdependencies with IT infrastructure needs

PC9. prioritize vulnerabilities based on business objectives, potential impact, and exploitability

Application Security Assessment and Vulnerability Management

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

PC10. secure infrastructure as code (IaC) templates (e.g., Terraform, CloudFormation) by identifying vulnerabilities, applying security best practices, and ensuring compliance with organizational security policies

PC11. utilize advanced vulnerability scanning tools such as Checkmarx, Veracode, or Snyk to identify security vulnerabilities in applications, analyze the results and mitigate risk

PC12. evaluate the security of containerized environments (e.g., Docker, Kubernetes) and implement measures to secure serverless functions (e.g., AWS Lambda, Azure Functions) to protect against vulnerabilities and threats

PC13. utilize PowerShell scripting to enhance application security

PC14. isolate root causes of vulnerabilities and identify fixes, by including contextual information like architectural composition, exploitation methods, and probabilities of exposure

PC15. verify data to detect false positives and isolate individual vulnerabilities

PC16. perform threat modeling to uncover potential vulnerabilities and implement security measures from the outset of software design and architecture

PC17. create an application tracking system to capture and record essential information

Comprehensive Application Security and Penetration Testing

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

PC18. develop a plan for application penetration testing that addresses multiple parameters

PC19. test applications using various testing methods

PC20. utilize malware sandboxing techniques to analyze and isolate potential threats

PC21. execute penetration testing by employing automated scanning technologies, black box testing, and manual tests that leverage human insight to inform the process

PC22. document the security requirements for applications specified by clients and external stakeholders in the designated format throughout the application life cycle

PC23. record information and activities at each stage to create a comprehensive audit trail

PC24. ensure the secure storage of data gathered during the assessment, including details on vulnerabilities, analysis findings, and mitigation recommendations

PC25. automate the integration of results from static, dynamic, and interactive application security testing

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. fundamentals of application security, including secure coding practices, authentication mechanisms, encryption techniques, and security frameworks.

KU2. various application penetration testing methodologies, including static application security testing (SAST), dynamic application security testing (DAST), and interactive application security testing (IAST).

KU3. API security principles, including authentication, authorization, rate limiting, data validation, and API gateway security measures.

KU4. industry-standard vulnerability assessment tools such as Checkmarx, Veracode, and Snyk, and their application in identifying, analyzing, and mitigating security risks.

KU5. Secure infrastructure as code (IaC) principles, ensuring security compliance for Terraform, CloudFormation, and Kubernetes configurations.

KU6. malware sandboxing techniques for detecting and isolating threats in applications and executing penetration testing using automated scanning technologies.

KU7. threat modeling methodologies to identify potential vulnerabilities and implement security measures during the software design and architecture phases.

KU8. best practices for maintaining and documenting security requirements, vulnerability reports, and mitigation measures throughout the application lifecycle.

Generic Skills (GS)

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

GS1. Analyze and interpret complex security data from vulnerability scanning tools to prioritize risks based on business impact and exploitability.

GS2. Apply critical thinking and problem-solving techniques to isolate root causes of vulnerabilities and recommend appropriate remediation strategies.

GS3. Utilize scripting languages such as PowerShell to automate security assessments and enhance application security operations.

GS4. Communicate effectively with stakeholders, including developers, security teams, and management, to ensure alignment on security requirements and mitigation strategies.

GS5. Maintain meticulous records of application assessments, penetration test results, and security compliance data for audit and regulatory purposes.

GS6. Adapt to emerging security threats, continuously updating knowledge on the latest attack vectors, security frameworks, and compliance standards.

GS7. Implement risk-based decision-making strategies, balancing security needs with business objectives to ensure optimal security measures.

GS8. Work efficiently in cross-functional teams, collaborating with developers, IT administrators, and cybersecurity professionals to enhance application security and maintain compliance.

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Application Security Assessment and Data Validation	**12**	**20**	**-**	**9**
PC1. review and collect initial information about the application from available data	2	2	-	1
PC2. assess the importance of information by considering multiple influencing factors like nature of the data, source of the data, size of the data and others	1	2	-	1
PC3. identify the application type/category by considering various factors like Programming languages, React, Angular, Spring frameworks and others	1	2	-	1
PC4. demonstrate the ability to assess and implement API authentication, authorization, rate limiting, and data validation to ensure secure and efficient API operations	2	2	-	1
PC5. conduct targeted assessments to validate and ensure the security of API operations, addressing vulnerabilities related to authentication, authorization, and data integrity	2	2	-	1
PC6. implement API gateway security measures, including rate limiting and authentication, to ensure secure and efficient API operations	1	2	-	1
PC7. assess applications to identify and address misconfigurations and supply chain vulnerabilities, ensuring alignment with security standards and best practices	1	2	-	1
PC8. collect data on application patching and its interdependencies with IT infrastructure needs	1	2	-	1
PC9. prioritize vulnerabilities based on business objectives, potential impact, and exploitability	1	4	-	1
Application Security Assessment and Vulnerability Management	**9**	**16**	**-**	**6**

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC10. secure infrastructure as code (IaC) templates (e.g., Terraform, CloudFormation) by identifying vulnerabilities, applying security best practices, and ensuring compliance with organizational security policies	1	3	-	1
PC11. utilize advanced vulnerability scanning tools such as Checkmarx, Veracode, or Snyk to identify security vulnerabilities in applications, analyze the results and mitigate risk	1	3	-	1
PC12. evaluate the security of containerized environments (e.g., Docker, Kubernetes) and implement measures to secure serverless functions (e.g., AWS Lambda, Azure Functions) to protect against vulnerabilities and threats	1	2	-	1
PC13. utilize PowerShell scripting to enhance application security	1	1	-	1
PC14. isolate root causes of vulnerabilities and identify fixes, by including contextual information like architectural composition, exploitation methods, and probabilities of exposure	1	2	-	-
PC15. verify data to detect false positives and isolate individual vulnerabilities	2	2	-	1
PC16. perform threat modeling to uncover potential vulnerabilities and implement security measures from the outset of software design and architecture	1	2	-	1
PC17. create an application tracking system to capture and record essential information	1	1	-	-
Comprehensive Application Security and Penetration Testing	**9**	**14**	**-**	**5**
PC18. develop a plan for application penetration testing that addresses multiple parameters	1	2	-	1
PC19. test applications using various testing methods	1	2	-	-
PC20. utilize malware sandboxing techniques to analyze and isolate potential threats	2	1	-	1

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC21. execute penetration testing by employing automated scanning technologies, black box testing, and manual tests that leverage human insight to inform the process	1	2	-	-
PC22. document the security requirements for applications specified by clients and external stakeholders in the designated format throughout the application life cycle	1	2	-	1
PC23. record information and activities at each stage to create a comprehensive audit trail	1	1	-	-
PC24. ensure the secure storage of data gathered during the assessment, including details on vulnerabilities, analysis findings, and mitigation recommendations	1	2	-	1
PC25. automate the integration of results from static, dynamic, and interactive application security testing	1	2	-	1
NOS Total	**30**	**50**	**-**	**20**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0958
NOS Name	Access API and application for security
Sector	IT-ITeS
Sub-Sector	
Occupation	Information and Cyber Security
NSQF Level	5
Credits	5
Version	1.0
Last Reviewed Date	18/02/2025
Next Review Date	18/02/2028
NSQC Clearance Date	18/02/2025

SSC/N0959: Manage application security, hardening and vulnerability

Description

The OS unit is about implementing security measures, hardening applications, and addressing vulnerabilities to protect systems from potential threats.

Scope

The scope covers the following :

- Web and Cloud Security Assessment and Hardening
- Threat Intelligence and Security Assessment for Emerging Technologies
- Implement and Maintain Application Security Measures

Elements and Performance Criteria

Web and Cloud Security Assessment and Hardening

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

PC1. locate all web servers and web applications on the network and secure their administrative interfaces

PC2. confirm that all web servers, web applications, and databases are updated with the latest patches and adhere to Security Technical Implementation Guides (STIGs) to ensure compliance with best practices

PC3. evaluate the list of systems and applications to identify and remove unauthorized instances and unnecessary functionalities to minimize the risk of exploitation

PC4. illustrate how Active Directory operates

PC5. detect and address attacks such as Kerberos ticket forging (Kerberos roasting)

PC6. apply hardening measures to strengthen domain controllers

PC7. review logs for web attacks and identify signs of compromise

PC8. implement application and database defenses such as firewalls

PC9. assess cloud platforms (AWS, Azure, GCP) along with their security features to protect internal servers of the organization

PC10. evaluate cloud infrastructure for potential vulnerabilities and verify that cloud environments comply with security best practices

Threat Intelligence and Security Assessment for Emerging Technologies

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

PC11. utilize threat intelligence to identify and respond to emerging threats

PC12. customize assessments according to current threat data

PC13. stay informed about the latest threat indicators

PC14. assess IoT devices and their applications for potential security vulnerabilities like lack of encryption, insecure software updates, lack of authentication and others

PC15. establish safeguards to protect communications between devices

PC16. evaluate the security of AI/ML models for vulnerabilities, biases, and potential adversarial attacks

PC17. ensure that cloud environments comply with security best practices and regularly evaluate and enhance the security posture using Cloud Security Posture Management (CSPM) tools

Implement and Maintain Application Security Measures

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

PC18. conduct fuzz testing to identify vulnerabilities in APIs and maintain ongoing monitoring for security breaches

PC19. work alongside development and operations teams to integrate security practices throughout the Software Development Life Cycle (SDLC) and automate security testing within Continuous Integration/Continuous Deployment (CI/CD) pipelines

PC20. review both frontend and backend platforms for identified vulnerabilities and assess available patches or updates

PC21. establish a security baseline for malware protection across servers, endpoints, and applications, ensuring regular signature updates and timely application of patch and security updates

PC22. collaborate with the application development team to identify, analyze, and mitigate security vulnerabilities, ensuring secure deployment and resolution of issues across the organization

PC23. educate business users on application vulnerabilities and the need for timely patching

PC24. ensure that IT infrastructure processes are redesigned to align with patch management requirements

PC25. investigate industry best practices for hardening applications to enhance security

PC26. record and document the outcomes generated by the tools and solutions implemented

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. The fundamentals of web server security, including hardening techniques, patch management, and Security Technical Implementation Guides (STIGs).

KU2. The structure and functioning of Active Directory, including security risks and mitigation strategies against attacks like Kerberos ticket forging (Kerberos roasting).

KU3. Threat intelligence methodologies to monitor, detect, and respond to emerging security threats effectively.

KU4. Cloud security principles and compliance best practices for platforms like AWS, Azure, and GCP, including Cloud Security Posture Management (CSPM) tools.

KU5. The role of firewalls, intrusion detection/prevention systems (IDS/IPS), and database security measures in protecting applications and infrastructure.

KU6. IoT security challenges, including encryption, authentication mechanisms, and software update best practices to mitigate potential vulnerabilities.

KU7. Secure Software Development Life Cycle (SDLC) and the importance of integrating security testing within Continuous Integration/Continuous Deployment (CI/CD) pipelines.

KU8. Security risks associated with AI/ML models, including bias, adversarial attacks, and ways to evaluate and mitigate vulnerabilities.

Generic Skills (GS)

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

GS1. Conduct security assessments of web applications, databases, and cloud infrastructure to identify vulnerabilities and compliance gaps.

GS2. Implement security configurations, patch management policies, and monitoring tools to maintain a strong security baseline across IT infrastructure.

GS3. Analyze threat intelligence reports and customize security assessments based on current threat landscapes.

GS4. Conduct fuzz testing and penetration testing on APIs and applications to identify and mitigate potential security risks.

GS5. Collaborate with cross-functional teams, including development and IT operations, to integrate security best practices into deployment and maintenance processes.

GS6. Educate business users and stakeholders on security best practices, vulnerability risks, and the importance of timely patch management.

GS7. Investigate and document security incidents, vulnerabilities, and remediation steps, ensuring detailed audit trails and compliance reporting.

GS8. Utilize automation tools to streamline security assessments, vulnerability scanning, and remediation processes for improved efficiency.

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Web and Cloud Security Assessment and Hardening	**10**	**20**	**-**	**8**
PC1. locate all web servers and web applications on the network and secure their administrative interfaces	1	2	-	1
PC2. confirm that all web servers, web applications, and databases are updated with the latest patches and adhere to Security Technical Implementation Guides (STIGs) to ensure compliance with best practices	1	2	-	-
PC3. evaluate the list of systems and applications to identify and remove unauthorized instances and unnecessary functionalities to minimize the risk of exploitation	1	2	-	1
PC4. illustrate how Active Directory operates	1	2	-	1
PC5. detect and address attacks such as Kerberos ticket forging (Kerberos roasting)	1	2	-	-
PC6. apply hardening measures to strengthen domain controllers	1	2	-	1
PC7. review logs for web attacks and identify signs of compromise	1	2	-	1
PC8. implement application and database defenses such as firewalls	1	2	-	1
PC9. assess cloud platforms (AWS, Azure, GCP) along with their security features to protect internal servers of the organization	1	2	-	1
PC10. evaluate cloud infrastructure for potential vulnerabilities and verify that cloud environments comply with security best practices	1	2	-	1
Threat Intelligence and Security Assessment for Emerging Technologies	**8**	**18**	**-**	**7**
PC11. utilize threat intelligence to identify and respond to emerging threats	1	2	-	1

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC12. customize assessments according to current threat data	1	2	-	1
PC13. stay informed about the latest threat indicators	1	3	-	1
PC14. assess IoT devices and their applications for potential security vulnerabilities like lack of encryption, insecure software updates, lack of authentication and others	1	3	-	1
PC15. establish safeguards to protect communications between devices	1	2	-	1
PC16. evaluate the security of AI/ML models for vulnerabilities, biases, and potential adversarial attacks	1	3	-	1
PC17. ensure that cloud environments comply with security best practices and regularly evaluate and enhance the security posture using Cloud Security Posture Management (CSPM) tools	2	3	-	1
Implement and Maintain Application Security Measures	**12**	**12**	**-**	**5**
PC18. conduct fuzz testing to identify vulnerabilities in APIs and maintain ongoing monitoring for security breaches	1	2	-	-
PC19. work alongside development and operations teams to integrate security practices throughout the Software Development Life Cycle (SDLC) and automate security testing within Continuous Integration/Continuous Deployment (CI/CD) pipelines	1	2	-	1
PC20. review both frontend and backend platforms for identified vulnerabilities and assess available patches or updates	1	1	-	-
PC21. establish a security baseline for malware protection across servers, endpoints, and applications, ensuring regular signature updates and timely application of patch and security updates	2	1	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC22. collaborate with the application development team to identify, analyze, and mitigate security vulnerabilities, ensuring secure deployment and resolution of issues across the organization	1	1	-	1
PC23. educate business users on application vulnerabilities and the need for timely patching	3	1	-	1
PC24. ensure that IT infrastructure processes are redesigned to align with patch management requirements	1	1	-	-
PC25. investigate industry best practices for hardening applications to enhance security	1	1	-	1
PC26. record and document the outcomes generated by the tools and solutions implemented	1	2	-	1
NOS Total	**30**	**50**	**-**	**20**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0959
NOS Name	Manage application security, hardening and vulnerability
Sector	IT-ITeS
Sub-Sector	
Occupation	Information and Cyber Security
NSQF Level	5
Credits	5
Version	1.0
Last Reviewed Date	18/02/2025
Next Review Date	18/02/2028
NSQC Clearance Date	18/02/2025

SSC/N0960: Oversee the Cloud security of deployed applications and solutions to detect potential breaches and compromises

Description

The OS unit is about monitoring cloud security for deployed applications and solutions to detect potential breaches and compromises, ensuring robust protection against cyber threats.

Scope

The scope covers the following :

- Application Security Monitoring and Threat Mitigation
- Threat Analysis, Incident Management, and Risk Mitigation

Elements and Performance Criteria

Application Security Monitoring and Threat Mitigation

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

PC1. confirm the scope of application assets and system components to be monitored with relevant authorized personnel

PC2. execute PowerShell syntax and basic commands effectively to automate tasks and enhance system administration

PC3. automate routine tasks and perform system administration efficiently by developing and executing security scripts using PowerShell

PC4. define and establish operational processes for log management

PC5. identify and capture all the key events and activity logs as per established format using appropriate tools and infrastructure

PC6. Conduct comprehensive security assessments of applications to identify vulnerabilities, assess potential risks, and ensure protection against threats such as hacking attempts, phishing, malware, and ransomware.

PC7. Implement and oversee security controls within software development to mitigate risks, ensuring that all applications adhere to industry security standards and protect against potential cyberattacks.

PC8. Perform real-time monitoring and threat analysis to detect and respond to security breaches, employing techniques to safeguard the organization from malware, ransomware, and other forms of cyber threats.

PC9. create secure sandbox environments to isolate threats

PC10. use sandbox environments to analyze malware behavior, detect malicious files, and assess associated risks

Threat Analysis, Incident Management, and Risk Mitigation

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

PC11. perform comprehensive analysis to uncover underlying security issues and implement long-term fixes and mitigation strategies to address identified vulnerabilities

PC12. collaborate with the organization’s computer network defense (CND) team to confirm network alerts

PC13. analyze the information collected to achieve situational awareness and assess the level of threat potential through event correlation

PC14. classify the urgency of recognized risks by assessing their likelihood of happening and potential consequences according to organizational procedures and policies

PC15. identify the necessary steps to assess and address recognized risks

PC16. log incidents in ticketing systems if any suspicious findings arise during the analysis

PC17. classify the service request according to the organization's processes and policies

PC18. allocate the ticket to the appropriate individuals based on the type of risk, in accordance with organizational procedures

PC19. arrange the service requests based on the organization's guidelines

PC20. coordinate with the appropriate personnel to ensure actions are taken on the tickets raised within the specified timelines

PC21. seek assistance or guidance from a specialist if the issue falls outside their knowledge or expertise

PC22. document the outcomes of monitoring, ticket creation, and ticket resolution activities using standardized forms in accordance with organizational protocols

PC23. adhere to applicable laws, regulations, policies, and guidelines

PC24. keep track of external data sources, such as CND vendor websites, Computer Emergency Response Teams, SANS, and Security Focus, to identify security issues that could affect the organization

PC25. conduct telemetry monitoring to detect issues with the security platform

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. The fundamental concepts of cybersecurity, including threat analysis, malware detection, incident management, and risk mitigation strategies.

KU2. The principles of log management, event correlation, and telemetry monitoring to identify security threats and anomalies in applications and systems.

KU3. The process of PowerShell scripting and automation techniques to streamline security operations, perform system administration, and manage cybersecurity tasks efficiently.

KU4. Industry security standards, regulatory requirements, and organizational security policies, including compliance with cybersecurity laws and guidelines.

KU5. The functionalities and application of sandbox environments to isolate and analyze malware, detect malicious files, and assess their impact on organizational security.

KU6. The different types of cyber threats such as phishing, hacking attempts, ransomware, and malware, along with appropriate preventive and response strategies.

KU7. The incident response lifecycle, including threat detection, classification, escalation procedures, ticketing systems, and risk assessment protocols.

KU8. The use of external cybersecurity data sources such as CND vendor websites, Computer Emergency Response Teams (CERTs), SANS, and Security Focus for tracking emerging threats.

Generic Skills (GS)

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

GS1. Execute PowerShell commands effectively to automate security tasks and enhance system administration.

GS2. Implement security assessments for applications and IT infrastructure, identifying vulnerabilities and ensuring compliance with security standards.

GS3. Perform real-time monitoring, analyze security logs, and correlate events to detect potential threats and security breaches.

GS4. Develop and maintain operational processes for logging key security events using appropriate tools and infrastructure.

GS5. Use sandboxing techniques to safely analyze malware behavior and evaluate potential security threats before they impact the system.

GS6. Log incidents accurately in ticketing systems, classify risks based on organizational policies, and escalate unresolved security issues to the appropriate teams.

GS7. Collaborate with cybersecurity and IT teams to implement and enforce security measures across software development and operational environments.

GS8. Document findings, generate security reports, and maintain compliance records to ensure transparency and alignment with cybersecurity regulations.

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Application Security Monitoring and Threat Mitigation	**15**	**20**	**-**	**9**
PC1. confirm the scope of application assets and system components to be monitored with relevant authorized personnel	1	2	-	1
PC2. execute PowerShell syntax and basic commands effectively to automate tasks and enhance system administration	2	2	-	-
PC3. automate routine tasks and perform system administration efficiently by developing and executing security scripts using PowerShell	2	2	-	1
PC4. define and establish operational processes for log management	2	2	-	1
PC5. identify and capture all the key events and activity logs as per established format using appropriate tools and infrastructure	2	2	-	1
PC6. Conduct comprehensive security assessments of applications to identify vulnerabilities, assess potential risks, and ensure protection against threats such as hacking attempts, phishing, malware, and ransomware.	1	2	-	1
PC7. Implement and oversee security controls within software development to mitigate risks, ensuring that all applications adhere to industry security standards and protect against potential cyberattacks.	1	2	-	1
PC8. Perform real-time monitoring and threat analysis to detect and respond to security breaches, employing techniques to safeguard the organization from malware, ransomware, and other forms of cyber threats.	1	2	-	1
PC9. create secure sandbox environments to isolate threats	1	2	-	1
PC10. use sandbox environments to analyze malware behavior, detect malicious files, and assess associated risks	2	2	-	1

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Threat Analysis, Incident Management, and Risk Mitigation	**15**	**30**	**-**	**11**
PC11. perform comprehensive analysis to uncover underlying security issues and implement long-term fixes and mitigation strategies to address identified vulnerabilities	2	2	-	1
PC12. collaborate with the organization’s computer network defense (CND) team to confirm network alerts	1	2	-	1
PC13. analyze the information collected to achieve situational awareness and assess the level of threat potential through event correlation	1	2	-	1
PC14. classify the urgency of recognized risks by assessing their likelihood of happening and potential consequences according to organizational procedures and policies	1	2	-	-
PC15. identify the necessary steps to assess and address recognized risks	1	2	-	1
PC16. log incidents in ticketing systems if any suspicious findings arise during the analysis	1	2	-	-
PC17. classify the service request according to the organization's processes and policies	1	2	-	-
PC18. allocate the ticket to the appropriate individuals based on the type of risk, in accordance with organizational procedures	1	2	-	1
PC19. arrange the service requests based on the organization's guidelines	1	2	-	1
PC20. coordinate with the appropriate personnel to ensure actions are taken on the tickets raised within the specified timelines	-	2	-	1
PC21. seek assistance or guidance from a specialist if the issue falls outside their knowledge or expertise	-	2	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC22. document the outcomes of monitoring, ticket creation, and ticket resolution activities using standardized forms in accordance with organizational protocols	1	2	-	1
PC23. adhere to applicable laws, regulations, policies, and guidelines	1	2	-	1
PC24. keep track of external data sources, such as CND vendor websites, Computer Emergency Response Teams, SANS, and Security Focus, to identify security issues that could affect the organization	2	2	-	1
PC25. conduct telemetry monitoring to detect issues with the security platform	1	2	-	1
NOS Total	**30**	**50**	**-**	**20**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N0960
NOS Name	Oversee the Cloud security of deployed applications and solutions to detect potential breaches and compromises
Sector	IT-ITeS
Sub-Sector	
Occupation	Information and Cyber Security
NSQF Level	5
Credits	5
Version	1.0
Last Reviewed Date	18/02/2025
Next Review Date	18/02/2028
NSQC Clearance Date	18/02/2025

DGT/VSQ/N0102: Employability Skills (60 Hours)

Description

This unit is about employability skills, Constitutional values, becoming a professional in the 21st Century, digital, financial, and legal literacy, diversity and Inclusion, English and communication skills, customer service, entrepreneurship, and apprenticeship, getting ready for jobs and career development.

Scope

The scope covers the following :

- Introduction to Employability Skills
- Constitutional values - Citizenship
- Becoming a Professional in the 21st Century
- Basic English Skills
- Career Development & Goal Setting
- Communication Skills
- Diversity & Inclusion
- Financial and Legal Literacy
- Essential Digital Skills
- Entrepreneurship
- Customer Service
- Getting ready for Apprenticeship & Jobs

Elements and Performance Criteria

Introduction to Employability Skills

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

PC1. identify employability skills required for jobs in various industries

PC2. identify and explore learning and employability portals

Constitutional values – Citizenship

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

PC3. recognize the significance of constitutional values, including civic rights and duties, citizenship, responsibility towards society etc. and personal values and ethics such as honesty, integrity, caring and respecting others, etc.

PC4. follow environmentally sustainable practices

Becoming a Professional in the 21st Century

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

PC5. recognize the significance of 21st Century Skills for employment

PC6. practice the 21st Century Skills such as Self-Awareness, Behaviour Skills, time management, critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn for continuous learning etc. in personal and professional life

Basic English Skills

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

PC7. use basic English for everyday conversation in different contexts, in person and over the telephone

PC8. read and understand routine information, notes, instructions, mails, letters etc. written in English

PC9. write short messages, notes, letters, e-mails etc. in English

Career Development & Goal Setting

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

PC10. understand the difference between job and career

PC11. prepare a career development plan with short- and long-term goals, based on aptitude

Communication Skills

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

PC12. follow verbal and non-verbal communication etiquette and active listening techniques in various settings

PC13. work collaboratively with others in a team

Diversity & Inclusion

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

PC14. communicate and behave appropriately with all genders and PwD

PC15. escalate any issues related to sexual harassment at workplace according to POSH Act

Financial and Legal Literacy

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

PC16. select financial institutions, products and services as per requirement

PC17. carry out offline and online financial transactions, safely and securely

PC18. identify common components of salary and compute income, expenses, taxes, investments etc

PC19. identify relevant rights and laws and use legal aids to fight against legal exploitation

Essential Digital Skills

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

PC20. operate digital devices and carry out basic internet operations securely and safely

PC21. use e- mail and social media platforms and virtual collaboration tools to work effectively

PC22. use basic features of word processor, spreadsheets, and presentations

Entrepreneurship

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

PC23. identify different types of Entrepreneurship and Enterprises and assess opportunities for potential business through research

PC24. develop a business plan and a work model, considering the 4Ps of Marketing Product, Price, Place and Promotion

PC25. identify sources of funding, anticipate, and mitigate any financial/ legal hurdles for the potential business opportunity

Customer Service

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

PC26. identify different types of customers

PC27. identify and respond to customer requests and needs in a professional manner.

PC28. follow appropriate hygiene and grooming standards

Getting ready for apprenticeship & Jobs

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

PC29. create a professional Curriculum vitae (Résumé)

PC30. search for suitable jobs using reliable offline and online sources such as Employment exchange, recruitment agencies, newspapers etc. and job portals, respectively

PC31. apply to identified job openings using offline /online methods as per requirement

PC32. answer questions politely, with clarity and confidence, during recruitment and selection

PC33. identify apprenticeship opportunities and register for it as per guidelines and requirements

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. need for employability skills and different learning and employability related portals

KU2. various constitutional and personal values

KU3. different environmentally sustainable practices and their importance

KU4. Twenty first (21st) century skills and their importance

KU5. how to use English language for effective verbal (face to face and telephonic) and written communication in formal and informal set up

KU6. importance of career development and setting long- and short-term goals

KU7. about effective communication

KU8. POSH Act

KU9. Gender sensitivity and inclusivity

KU10. different types of financial institutes, products, and services

KU11. how to compute income and expenditure

KU12. importance of maintaining safety and security in offline and online financial transactions

KU13. different legal rights and laws

KU14. different types of digital devices and the procedure to operate them safely and securely

KU15. how to create and operate an e- mail account and use applications such as word processors, spreadsheets etc.

KU16. how to identify business opportunities

KU17. types and needs of customers

KU18. how to apply for a job and prepare for an interview

KU19. apprenticeship scheme and the process of registering on apprenticeship portal

Generic Skills (GS)

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

GS1. read and write different types of documents/instructions/correspondence

GS2. communicate effectively using appropriate language in formal and informal settings

GS3. behave politely and appropriately with all

GS4. how to work in a virtual mode

GS5. perform calculations efficiently

GS6. solve problems effectively

GS7. pay attention to details

GS8. manage time efficiently

GS9. maintain hygiene and sanitization to avoid infection

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Introduction to Employability Skills	**1**	**1**	**-**	**-**
PC1. identify employability skills required for jobs in various industries	-	-	-	-
PC2. identify and explore learning and employability portals	-	-	-	-
Constitutional values – Citizenship	**1**	**1**	**-**	**-**
PC3. recognize the significance of constitutional values, including civic rights and duties, citizenship, responsibility towards society etc. and personal values and ethics such as honesty, integrity, caring and respecting others, etc.	-	-	-	-
PC4. follow environmentally sustainable practices	-	-	-	-
Becoming a Professional in the 21st Century	**2**	**4**	**-**	**-**
PC5. recognize the significance of 21st Century Skills for employment	-	-	-	-
PC6. practice the 21st Century Skills such as Self-Awareness, Behaviour Skills, time management, critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn for continuous learning etc. in personal and professional life	-	-	-	-
Basic English Skills	**2**	**3**	**-**	**-**
PC7. use basic English for everyday conversation in different contexts, in person and over the telephone	-	-	-	-
PC8. read and understand routine information, notes, instructions, mails, letters etc. written in English	-	-	-	-
PC9. write short messages, notes, letters, e-mails etc. in English	-	-	-	-
Career Development & Goal Setting	**1**	**2**	**-**	**-**

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC10. understand the difference between job and career	-	-	-	-
PC11. prepare a career development plan with short- and long-term goals, based on aptitude	-	-	-	-
Communication Skills	**2**	**2**	**-**	**-**
PC12. follow verbal and non-verbal communication etiquette and active listening techniques in various settings	-	-	-	-
PC13. work collaboratively with others in a team	-	-	-	-
Diversity & Inclusion	**1**	**2**	**-**	**-**
PC14. communicate and behave appropriately with all genders and PwD	-	-	-	-
PC15. escalate any issues related to sexual harassment at workplace according to POSH Act	-	-	-	-
Financial and Legal Literacy	**2**	**3**	**-**	**-**
PC16. select financial institutions, products and services as per requirement	-	-	-	-
PC17. carry out offline and online financial transactions, safely and securely	-	-	-	-
PC18. identify common components of salary and compute income, expenses, taxes, investments etc	-	-	-	-
PC19. identify relevant rights and laws and use legal aids to fight against legal exploitation	-	-	-	-
Essential Digital Skills	**3**	**4**	**-**	**-**
PC20. operate digital devices and carry out basic internet operations securely and safely	-	-	-	-
PC21. use e- mail and social media platforms and virtual collaboration tools to work effectively	-	-	-	-
PC22. use basic features of word processor, spreadsheets, and presentations	-	-	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Entrepreneurship	**2**	**3**	**-**	**-**
PC23. identify different types of Entrepreneurship and Enterprises and assess opportunities for potential business through research	-	-	-	-
PC24. develop a business plan and a work model, considering the 4Ps of Marketing Product, Price, Place and Promotion	-	-	-	-
PC25. identify sources of funding, anticipate, and mitigate any financial/ legal hurdles for the potential business opportunity	-	-	-	-
Customer Service	**1**	**2**	**-**	**-**
PC26. identify different types of customers	-	-	-	-
PC27. identify and respond to customer requests and needs in a professional manner.	-	-	-	-
PC28. follow appropriate hygiene and grooming standards	-	-	-	-
Getting ready for apprenticeship & Jobs	**2**	**3**	**-**	**-**
PC29. create a professional Curriculum vitae (Résumé)	-	-	-	-
PC30. search for suitable jobs using reliable offline and online sources such as Employment exchange, recruitment agencies, newspapers etc. and job portals, respectively	-	-	-	-
PC31. apply to identified job openings using offline /online methods as per requirement	-	-	-	-
PC32. answer questions politely, with clarity and confidence, during recruitment and selection	-	-	-	-
PC33. identify apprenticeship opportunities and register for it as per guidelines and requirements	-	-	-	-
NOS Total	**20**	**30**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	DGT/VSQ/N0102
NOS Name	Employability Skills (60 Hours)
Sector	Cross Sectoral
Sub-Sector	Professional Skills
Occupation	Employability
NSQF Level	4
Credits	2
Version	1.0
Last Reviewed Date	30/04/2025
Next Review Date	30/04/2028
NSQC Clearance Date	30/04/2025

Assessment Guidelines and Assessment Weightage

Assessment Guidelines

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

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

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

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

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

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

7. Candidate needs to achieve 70% or more for successfully passing the QP.

Minimum Aggregate Passing % at QP Level : 70

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

Assessment Weightage

Compulsory NOS

National Occupational Standards	Theory Marks	Practical Marks	Project Marks	Viva Marks	Total Marks	Weightage
SSC/N0958.Access API and application for security	30	50	0	20	100	28
SSC/N0959.Manage application security, hardening and vulnerability	30	50	0	20	100	28
SSC/N0960.Oversee the Cloud security of deployed applications and solutions to detect potential breaches and compromises	30	50	0	20	100	28
DGT/VSQ/N0102.Employability Skills (60 Hours)	20	30	-	-	50	16
Total	**110**	**180**	**-**	**60**	**350**	**100**

Acronyms

NOS	National Occupational Standard(s)
NSQF	National Skills Qualifications Framework
QP	Qualifications Pack
TVET	Technical and Vocational Education and Training

Glossary

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

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