Model Curriculum

Analyst Application Security

SECTOR: IT-ITeS

SUB-SECTOR: IT Services

OCCUPATION: Information/Cyber Security

REF ID: SSC/Q0903

NSQF LEVEL: 7

TABLE OF CONTENTS

1. Curriculum..... 01

2. Trainer Prerequisites..... 07

3. Annexure: Assessment Criteria..... 08

Analyst Application Security

CURRICULUM / SYLLABUS

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

Program Name	**Analyst Application Security**		
Qualification Pack Name & Reference ID. ID	**Analyst Application Security** **SSC/Q0903**		
Version No.	1.0	**Version Update Date**	04/11/2016
Pre-requisites to Training	• Diploma in Engineering (with 1 year experience) or Bachelor's Degree in Science/Technology/Computers		
Minimum Job Entry Age	• 21 years		
Training Outcomes	**After completing this programme, participants will be able to:** **1.** SSC/N0909 (Identify and analyze exposures and weaknesses in applications and their deployments) **2.** SSC/N0910 (Harden application and deployment configurations for minimizing exposure and vulnerabilities) **3.** SSC/N0911 (Monitor applications and solutions deployed for possible breaches and compromises) **4.** SSC/N9001 (Manage your work to meet requirements) **5.** SSC/N9002 (Work effectively with colleagues) **6.** SSC/N9003 (Maintain a healthy, safe and secure working environment) **7.** SSC/N9004 (Provide data/information in standard formats) **8.** SSC/N9005 (Develop your knowledge, skills and competence)		

This course encompasses 8 out of 8 National Occupational Standards (NOS) of "Analyst Application Security" Qualification Pack issued by "IT-ITeS SSC".

Sr. No.	Module	Key Learning Outcomes	Equipment Required
1	**IT-ITES/BPM Industry – An Introduction** **Theory Duration** (hh:mm) 6:00 **Practical Duration** (hh:mm) 03:00 **Corresponding NOS Code** The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.	• Explain relevance of the IT-ITES industry • State the various sub-sectors in the IT-ITES sector • Explain the relevance of IT services sector • A General Overview of the IT-BPM Industry • The organisations within IT-BPM Industry • The sub-sectors within the IT BPM Industry	• Whiteboard and Markers • LCD Projector and Laptop for presentations • Lab equipped with the following: • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated) • Networking Equipment-Routers & Switches • Chart paper and sketch pens
2	**IT Services – An Introduction** **Theory Duration** (hh:mm) 01:00 **Practical Duration** (hh:mm) 01:00 **Corresponding NOS Code** The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.	• State the various occupations and tracks in the IT-ITES sector • General Overview of the IT Services Sub-Sector • Profile of the IT Services Sub-Sector • Key Trends in the IT Services Sub-Sector • Roles in the IT Services Sub-Sector	• Whiteboard and Markers • LCD Projector and Laptop for presentations • Lab equipped with the following: • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated)
3	**Information/Cyber Security – An Introduction** **Theory Duration** (hh:mm)	• Explain the relevance of cyber security in the society • Explain the role of an Analyst – Application Security and their key responsibilities • List the range of skills and	• Lab equipped with the following: • PCs/Laptops • Internet with WiFi (Min 2 Mbps Dedicated)

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	03:00 **Practical Duration** (hh:mm) 02:00 **Corresponding NOS Code** The introduction is not based on any NOS, however is important in order to understand the context of the course and the role.	behavior, expected from Analyst – Application Security • List the responsibilities of an Analyst – Application Security • State the growth opportunities for an Analyst – Application Security • General Overview of Information/cyber security and its Roles • Career Map for Information/cyber security	• Whiteboard and Markers • Chart paper and sketch pens
4	**Fundamental Concepts** **Theory Duration** (hh:mm) 09:00 **Practical Duration** (hh:mm) 32:00 **Corresponding NOS Code** SSC/N0909	• relevant networking concepts, devices and terminologies • standard Systems Development Lifecycle (SDLC) practices and process • basic cyber security concepts • the enterprise information technology (IT) architecture Information Technology Architecture • what are applications, types of applications and common application security requirements • the basic functionalities of the applications, hardware and/or access rights that are used by the customers • application / database layer intrusion detection / prevention appliance	• Whiteboard and Markers • LCD Projector and Laptop for presentations • Lab with • key devices, software and hardware in a large network. • Should include but not be limited to- application of multiple networking topology; use of various Network Protocols; bandwidth management tools; application of host network access controls; hubs; switches; routers; bridges; servers; transmission media IDS/IPS; application of SSL, VPN, 2FA, Encryption, etc.
5	**Application vulnerabilities** **Theory Duration** (hh:mm) 08:00 **Practical Duration** (hh:mm) 25:00	• explain what applications are • state key vulnerabilities to applications • explain overall process of identification of these vulnerabilities • explain how hardware and software vulnerabilities can be identified and resolved • describe application/ database	• Whiteboard and markers • LCD projector and laptop for presentations • Access to various samples of applications of each category including various types of computer applications, mobile

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	Corresponding NOS Code SSC/N0909	layer intrusion detection/ prevention appliance	applications and cloud applications. • Provision for online research in the lab for all students • At least two subject matter experts from the industry in the field of application security • Samples of secure applications and open source code scanning tools.
6	**Identification of Vulnerabilities** **Theory Duration** (hh:mm) 03:00 **Practical Duration** (hh:mm) 08:00 **Corresponding NOS Code** SSC/N0909	• View the system as an adversary ○ gather preliminary information about an application through manual documentation review ○ gather web based information through the use of automated tools and techniques ○ check the source code of a web application manually for security issues ○ collate application information security controls from various internal and external sources ○ collate information about an application with respect to industry trends through various sources ○ gather information related to application patching and its interdependencies with IT infrastructure requirements. ○ describe and use code scanning toolsets, such as Fortify and Ounce • Characterise the system ○ evaluate the criticality of information by taking into	• Whiteboard and markers • LCD projector and laptop for presentations • Provision for online research in the lab for all students • Access to various samples of applications of each category including various types of computer, mobile, and cloud applications • Samples of secure applications • Open source code scanning tools and their tutorials • Access to secure and unsecured applications for practicing penetration testing activities • Access to public databases and vulnerability sharing clubs, e.g., • Bugtraq • National Institute of Standards and Technology (NIST) NVB, • United States Computer Emergency Readiness Team (US-CERT),

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		consideration various factors ○ identify the application type/ category by considering various factors ○ identify the dependency an application has with in-house/ outsourced/ third party/ client applications ○ establish the application functionality and connectivity, and understand how it works ○ review application design and architecture to ensure that appropriate security requirements are enforced ○ explore potential threats by using threat scenarios from various sources • Modelling the system ○ explore potential threats by using threat scenarios from various sources ○ efficiently isolate root causes and identify fixes by including contextual information, like architectural composition, exploitation methods, and probabilities of exposure ○ develop an application tracker with respect to risk exposure, and any application deficiency identified in the past capturing relevant information ○ validate data to identify false positives and individual vulnerabilities ○ categorise vulnerabilities and identify extent of vulnerability including level of weakness and	• Open Source Vulnerability Database (OSVDB), etc.

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		sensitivity of information ○ identify the root cause of vulnerabilities ○ evaluate vulnerabilities that are discovered from their relevance, root causes, risk criticality, and corresponding mitigation methods based various factors • Application penetration testing ○ plan for penetration testing covering various parameters ○ test applications using various testing methods ○ use automatic scanning technologies 'black box testing' that sends malformed inputs to an application and scrutinises responses for vulnerabilities and unexpected behaviour ○ conduct manual tests that use human intelligence to guide the penetration steps can uncover hard-to-locate errors, and often more accurately reflect actions of an actual attacker ○ capture the needs and requirements required to secure applications in designated format during the application life cycle ○ capture application security requirements stipulated by clients and external stakeholders ○ document the security requirements in a structured report for easy reference and knowledge ○ document information and activities at every step to	

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		provide an audit trail ○ secure storage of data collected during the assessment, including vulnerabilities, analysis results, and mitigation recommendations • use tools that focus on protocol penetration testing	
7	**Threat/ Vulnerability Analysis** **Theory Duration** (hh:mm) 03:00 **Practical Duration** (hh:mm) 08:00 **Corresponding NOS Code** SSC/N0909	• Efficiently isolate root causes and identify fixes by including contextual information, like architectural composition, exploitation methods, and probabilities of exposure • Develop an application tracker with respect to risk exposure, and any application deficiency identified in the past capturing relevant information • Validate data to identify false positives and individual vulnerabilities • Categorise vulnerabilities and identify extent of vulnerability including the level of weakness and sensitivity of information • Identify the root cause of vulnerabilities • Evaluate vulnerabilities that are discovered from their relevance, root causes, risk criticality, and corresponding mitigation methods based on various factors • Capture application security requirements stipulated by clients and external stakeholders • Document security requirements in a structured report for easy reference and knowledge • Document information and activities at every step to provide an audit trail • Secure storage of data collected during the assessment, including	• Whiteboard and markers • LCD projector and laptop for presentations • Provision for online research in the lab for all students • Access to list of vulnerabilities and exposures identified in the application by participants in the activities of previous topic. • Open source tools in the for the above-mentioned activities • Provision for online research for all participants • Sample templates for the above-mentioned points • Provision of software, such as word processors, spreadsheets, etc. for preparing reports for all participants.

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		vulnerabilities, analysis results, and mitigation recommendations	
8	**Cyber Security Policies, Procedures, Standards & Guidelines** **Theory Duration** (hh:mm) 07:00 **Practical Duration** (hh:mm) 20:00 **Corresponding NOS Code** SSC/N0909	• relevant legislation, standards, policies, and procedures followed in a company • organisational systems, procedures and tasks/ checklists within the domain and how to use the same • operating procedures that are applicable to the system(s) being used, typical response times and service times related to own work area • OWASP tools and methodologies • standard tools and templates available and how to use the same	• Whiteboard and markers • LCD projector and laptop for presentations • Provision for online research in the lab for all students • Access to free OWASP tools and methods and their tutorials • Around 2-3 computer applications, 2-3 mobile applications and 2-3 web applications
9	**Technological Developments in Application Security** **Theory Duration** (hh:mm) 05:00 **Practical Duration** (hh:mm) 14:00 **Corresponding NOS Code** SSC/N0909	• importance of technological upgradation in cyber security • next generation techniques for controlling advanced threats to applications • improved ways of preventing remote applications by being compromised	• Whiteboard and markers • LCD projector and laptop for presentations • Provision for online research in lab for all students • Access to free OWASP tools and methods and their tutorials • Around 2-3 computer applications, 2-3 mobile applications and 2-3 web applications
10	**Fundamental Concepts** **Theory Duration** (hh:mm) 07:00 **Practical Duration** (hh:mm)	• Identify all web servers and web applications on a network • Work on various operating systems • Work with word processors, spreadsheets and presentations • Do HTTP and web programming • Read and write coded scripts	• Whiteboard and markers • LCD projector and laptop for presentations • Lab with provision for online research • Lab with web application servers and web applications on the network • One open source software,

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	30:00 **Corresponding NOS Code** SSC/N0910	and modify and debug programmes • Basic cyber security concepts • Relevant networking concepts, devices and terminologies • Standard Systems Development Life Cycle (SDLC) practices and process • Enterprise information technology (IT) architecture • Organisation's knowledge base and how to access and update the same • What are applications, types of applications and common security requirements • Basic functionalities of applications, hardware and/or access rights • How hardware and software vulnerabilities can be identified and resolved for applications • Application/ database layer intrusion detection/ prevention appliance • CVE language, which standardises descriptions of vulnerabilities • Security solutions like Firewall, IDS/IPS, web security gateways, email security, content management, etc. • Relevant legislation, standards, policies, and procedures followed in a company • Limits of one's role and responsibilities and who to seek guidance from • Organisational systems, procedures and tasks/checklists	such as Django, Drupal, Ruby on Rails or Symfony called web application frameworks for writing applications

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		within the domain and how to use the same • Operating procedures that are applicable to the system(s) being used, typical response times and service times related to own work area	
11	**Application Hardening** **Theory Duration (hh:mm)** 03:00 **Practical Duration (hh:mm)** 09:00 **Corresponding NOS Code** SSC/N0910	• About Application Hardening • Application Hardening processes	• Whiteboard and markers • LCD projector and laptops for making presentations
12	**Configuration Management** **Theory Duration** (hh:mm) 06:00 **Practical Duration** (hh:mm) 23:00 **Corresponding NOS Code** SSC/N0910	• Configure application securely across environments for minimum exposure and weaknesses • Configuration management • Secure configuration of applications +	• Whiteboard and markers • Provision for online research in lab • LCD projector and laptops for making presentations
13	**Web Application Secure Configuration** **Theory Duration** (hh:mm) 06:00 **Practical Duration** (hh:mm)	• configure web applications securely across environments for minimum exposure and weaknesses • secure applications using tools and solutions, such as application testing, code review, web application firewall, etc. • do HTTP and web programming	• Whiteboard and markers • Lab with software and tools for writing secure web application configurations • Sample secure web application configurations

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	20:00 **Corresponding NOS Code** SSC/N0910	• read and write coded scripts and modify and debug programmes	
14	**Patch Management** **Theory Duration (hh:mm)** 08:00 **Practical Duration (hh:mm)** 30:00 **Corresponding NOS Code** SSC/N0910	• ensure all web servers, web applications and databases are patched as per latest guidelines • check frontend and backend platforms for reported vulnerabilities and available patches or updates • establish a mechanism to ensure that security updates and patches are applied on all application assets. This will help to close out issues or weaknesses that appear in the operational life cycle of an asset. • establish measures for effectively patching an application, making business users aware about application vulnerability and patch requirements • define strategy for management of patches and updates considering various relevant factors • identify a patch management life cycle process considering various parameters • integrate patch management with operational cycle of IT infrastructure management • ensure that IT infrastructure processes are reengineered as per patch management requirements	• Whiteboard and markers • Provision for online research in lab • Sample patches • Lab with key devices, software and hardware in a large network
15	**Monitoring and Logging of**	• verify scope of application assets and system components to be	• Whiteboard and markers

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	Application Events and Alarms **Theory Duration** (hh:mm) 27:00 **Practical Duration** (hh:mm) 73:00 **Corresponding NOS Code** SSC/N0911	monitored with authorised persons • use specified monitoring and data collection methods and tools following organisational procedures and policies • monitor application consoles using Security Information and Event Management (SIEM) tool to detect security threats and health of applications • define and establish operational processes for log management • • identify and capture all key events and activity logs as per established format using appropriate tools and infrastructure • ensure that mechanisms, such as time stamping and synchronisation of servers are utilised for time consistency among all log sources • maintain a tracker which captures inventory of incidents related to applications • define in co-ordination with seniors and incident management team process for incident/breach management plan and technical and tactical measures deployed to detect or report incidents • work on defined process for prioritisation and handling of incidents • characterise and analyse application traffic to identify anomalous activity and potential	• Lab and access to SIEM tool and online tutorials. List of tasks that have to be performed

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		threats • identify trends and patterns as per standard guidelines • coordinate with enterprise wide computer network defence (CND) staff to validate network alerts • perform event correlation using information gathered to gain situational awareness and determine threat potential • categorise priority of identified risks by determining their probability of occurrence and potential impact as per organisational processes and policies • determine actions required to investigate and mitigate identified risks • raise incidents in ticketing tools if something is found suspicious during the analysis • record and categorise service request accurately as per organisational processes and policies • assign ticket to relevant persons as per the type of risk following organisational procedures • prioritise service request according to organisational guidelines • follow-up with relevant personnel for taking actions on tickets raised within agreed timelines • obtain help or advice from specialist if problem is outside his/her area of competence or	

Sr. No.	Module	Key Learning Outcomes	Equipment Required
		experience • report results of monitoring, ticket raising and ticket closure activities using standard documentation following organisational procedures • comply with relevant legislation, standards, policies and procedures • monitor external data sources (e.g., computer network defence [CND] vendor sites, Computer Emergency Response Teams, SANS& Security Focus) and determine which security issues may have an impact on enterprise • perform telemetry monitoring to identify security platform issues	
16	**Manage your work to meet requirements** **Theory Duration** (hh:mm) 12:00 **Practical Duration** (hh:mm) 38:00 **Corresponding NOS Code** SSC/N9001	• Understanding scope of work and working within limits of authority • Work and work environment • Maintaining Confidentiality	• Whiteboard and Markers • LCD Projector and Laptop for presentations • Training organization's confidentiality policy
17	**Work effectively with colleagues** **Theory Duration** (hh:mm) 12:00 **Practical Duration** (hh:mm)	• Effective Communication • Working Effectively	• Whiteboard and Markers • LCD Projector and Laptop for presentations • Provision to write emails and send in the lab • Lab with provision for internet, email, word processor and presentation

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	38:00 **Corresponding NOS Code** SSC/N9002		software • Chart paper, markers, picture magazines and old newspapers
18	**Maintain a healthy, safe and secure working environment** **Theory Duration** (hh:mm) 06:00 **Practical Duration** (hh:mm) 19:00 **Corresponding NOS Code** SSC/N9003	• Need for Health and Safety at Work • Analyst's Role • Emergency Situations • Skills for Maintaining Health and Safety at Work	• Whiteboard and Markers • LCD Projector and Laptop for presentations • The training organization's current health, safety and security policies and procedures • Provision for online research in the Lab • A sample health and safety policy document • Emergency broadcast system and mock emergency signage in the appropriate areas of the training institute
19	**Provide data/information in standard formats** **Theory Duration** (hh:mm) 12:00 **Practical Duration** (hh:mm) 38:00 **Corresponding NOS Code** SSC/N9004	• Information and Knowledge Management • How to manage data/ information effectively • Skills required to manage data and information effectively	• Whiteboard and Markers • LCD Projector and Laptop for presentations • Provision for online research in the lab
20	**Develop knowledge, skills and competence** **Theory Duration** (hh:mm) 06:00 **Practical Duration**	• Importance of self-development • Knowledge and Skills required for the job • Avenues for Self-Development • Planning for Self-Development	Whiteboard and Markers • LCD Projector and Laptop for presentations • Soft copy of QP-NOS • Provision for online access to all students in the lab Questionnaire and key for Honey and Mumford learning styles

Sr. No.	Module	Key Learning Outcomes	Equipment Required
	(hh:mm) 19:00 **Corresponding NOS Code** SSC/N9005		

	Total Duration: **Theory Duration (hh:mm)** **150:00** **Practical Duration (hh:mm)** **450:00**

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

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

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

Sr. No.	Area	Details
1	**Description**	**To deliver accredited training service, mapping to the curriculum detailed above, in accordance with the Qualification Pack SSC/Q0903.**
2	**Personal Attributes**	**Aptitude for conducting training, and pre/ post work to ensure competent, employable candidates at the end of the training. Strong communication skills, interpersonal skills, ability to work as part of a team; a passion for quality and for developing others; well-organized and focused, eager to learn and keep oneself updated with the latest in this field.**
3	**Minimum Educational Qualifications**	**Diploma in Engineering(with 1 year experience) or Bachelor's Degree in Science/Technology/Computers**
4a	**Domain Certification**	**2 years of work/training experience with respect to QP/Occupation 80% marks achieved in QP /NOS assessment (i.e. aggregate- 80% & per NOS - 70%) Additional certification in customer orientation, dealing with difficult customers, written communication etc. will be an added advantage.**
4b	**Platform Certification**	**80% marks achieved in Trainer QP (MEP/0102)/TVET/ pedagogy assessments (i.e. aggregate- 80% & per NOS - 70%)**
5	**Experience**	**Field experience: Minimum 2 years' experience in the same domain Training experience: 1 year preferred**

Annexure: Assessment Criteria

Criteria for Assessment of Trainees

Job Role Analyst Application Security

Qualification Pack SSC/Q0903

Sector Skill Council IT-ITeS

Guidelines for Assessment:

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

Title of NOS/Unit/Component:

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

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

	PC21. capture the requirements for securing applications stipulated by clients & external stakeholders in designated format during the application life cycle		4	1	3
	PC22. document information and activities at every step to provide an audit trail		4	2	2
	PC23. secure storage of data collected during the assessment, including vulnerabilities, analysis results, and mitigation recommendations		4	1	3
	PC24. automate correlation of static, dynamic and interactive application security testing results		4	1	3
		Total	**100**	**31**	**69**
2. SSC/N0910 (Harden application and deployment configurations for minimizing exposure and vulnerabilities)	PC1. identify all web servers and web applications on the network and secure their administrative consoles	**100**	4	1	3
	PC2. review the list of all applications and ensure valid credentials are required to connect		3	1	2
	PC3. review list of systems and applications to identify and uninstall unauthorized instances and extraneous functionality to reduce the chance of exploitation		3	1	2
	PC4. apply access controls to applications and databases as required as per policy		5	1	4
	PC5. ensure all web servers, web applications and databases are patched as per latest guidelines		4	1	3
	PC6. ensure all follow security technical implementation guides (STIGs) to ensure compliance with best practices		3	1	2
	PC7. review logs for web attacks and identify signs of compromise		4	1	3
	PC8. implement application and database defenses such as firewalls		6	2	4
	PC9. ensure that all applications connect with least privilege		4	1	3

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

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

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

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

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

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