GUJARAT TECHNOLOGICAL UNIVERSITY

Syllabus for Bachelor of Vocation (B.Voc), 5th Semester
Branch: Software Development
Subject Name: On-Job Training (Elective): Consultant Network Security
Subject Code: 1150209

With effective from academic year 2018-19

Type of course: On-Job Training (Elective)
Prerequisite: NA
Rationale:- On-job training, also known as OJT, is a hands-on method of teaching the skills, knowledge, and competencies needed for students to perform a specific task within the workplace. Students learn in an environment where they will need to practice the knowledge and skills obtained during their training.

Teaching and Examination Scheme:

Teaching Scheme			Credit	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA(M)	ESE (V)	PA(I)	
0	0	15	15	0	0	100	100	200

L- Lectures; T- Tutorial/Teacher Guided Student Activity; P- Practical; C- Credit; ESE- End Semester Examination; PA- Progressive Assessment

OJT Hands on Exercise/Training:

Sr. No.	Training / Hands on Exercise	Hrs.
1	**Provide network security recommendations as per requirements** PC1. Consult with customers to evaluate functional requirements for network security. PC2. Define project scope and objectives based on customer requirements. PC3. Confirm availability of complete and accurate details of the security objectives. PC4. Evaluate the existing network protocols and topology of users. PC5. Review the usage of existing network security measures, and assess risks w.r.t security objectives. PC6. Consult with engineering teams engaged in IT networking and network security to identify network security vulnerabilities and requirements. PC7. Conduct technical risk analysis, threat identification of the existing network security measures. PC8. Identify level of risk acceptable for business requirements by discussing with business and technical leads. PC9. Critically interpret information and data, from both within the customer/client organization and other sources, in order to identify network security requirements. PC10. Research relevant information required to meet the security objectives based on the evaluation of assets, threats, vulnerabilities and security risks. PC11. Identify and record details of constraints that may have an impact on the business and security options. PC12. Explore potential vulnerabilities that could be technical, operational or management related. PC13. Categorize vulnerabilities and identify extent of vulnerability including level of weakness and sensitivity of the information. PC14. Identify the root cause of vulnerabilities. PC15. Research options of network security solutions that match the productivity and security requirements captured. PC16. Gather sufficient accurate information on which to determine potential costs,	40

	benefits and effectiveness of potential security solutions. PC17. Identify and determine the cost, potential benefits, and effectiveness of recommended security solutions, based on valid assumptions, considerations and information, including possible constraints. PC18. Prepare recommendations that have the potential to meet the security objectives of the organization. PC19. Provide details of costs, benefits, effectiveness, limitations and constraints of recommendations. PC20. Provide recommendations of security solutions in an agreed format to the responsible person within agreed timescales. PC21. Provide the organization with considered advice on the implications of accepting, modifying or rejecting security recommendations. PC22. Co-ordinate with respective equipment manufacturer or solution providers for troubleshooting and enhancements to existing solutions as per business needs. PC23. Take account of the organization's values, culture and nature of business. PC24. Maintain the security and confidentiality of information relating to your organization and recommendations. PC25. Obtain necessary approvals from the responsible persons as per organizational policy. PC26. Evaluate ways and means of closing weaknesses in the network. PC27. Maintain logs for all the activities performed.	
2	**Carry out configuration review and provide recommendations for secure configuration of networks and security devices** PC1. Conduct an inventory to identify the information security devices that need to be protected. PC2. Characterize network resources deployed into publicly available databases and customer-facing systems, resources that have high concentrations of sensitive data, and legacy security devices. PC3. Identify and record the configurations of network configuration items that impact the cyber security posture of the organization. PC4. Review initial configuration of network configuration items considering security vulnerabilities and threats identified. PC5. Provide recommendations for secure configuration measures for networks considering business requirements. PC6. Establish a baseline configuration that represents a secure state which is also cost-effective as supportive of business requirements. PC7. Provide recommendation for secure configuration policies and procedures in alignment to cyber security posture of the organization and business requirements. PC8. Provide recommendation of appropriate solution for secure configuration management (SCM solution) as per requirements of the organization. PC9. Test secure configurations prior to implementation in the production environment. PC10. Diagnose issues and respond to queries from the implementation team with respect to various secure configuration processes and specifications. PC11. Suggest remediation actions to resolve issues caused due to erroneous network device configurations.	40
3	**Test, run exploits to identify vulnerabilities in networks** PC1. Gather preliminary information by manually reviewing the documentation, secure	40

	coding policies, security requirements, and architectural designs. PC2. Gather network information using various information gathering methods and tools. PC3. Define scope for the tests using Existing Security Policies and Industry Standards. PC4. Plan for the test while adhering to business and time constraints put by organization. PC5. Perform Active Reconnaissance on the target network using metadata, search engines, social engineering, dumpster diving etc. After takingadequate approvals. PC6. Develop a map of target environments. PC7. Utilize network infrastructure scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting and version scanning. PC8. Identify live systems, open / filtered ports found, services running on these ports, mapping router / firewall rules, operating system details, network path discovery, etc. PC9. Perform fingerprinting services running behind open ports and underlying operating system. PC10. Explore the network by pre-determined scans to find possible vulnerabilities. PC11. Perform social engineering using Social Engineering Toolkit (SET) to find possible security holes. PC12. Test the network devices by supplying invalid inputs, random strings, etc., and check for any errors or unintended behavior in the output. PC13. Find exploits e.g. proof-of-concept exploit for the various vulnerabilities found. PC14. Identify weak entry points and high value target assets of the organization or its network. PC15. Identify antiviruses' e.g. Host-based intrusion prevention systems, web application firewalls, and other preventative technologies in the system. PC16. Use pivoting techniques through targeted systems. PC17. Demonstrate various possible impacts, compromises and exposures using specialized exploitation tools. PC18. Evaluate ways and means of identifying and closing weaknesses in the network. PC19. Maintain logs for all the activities performed.	
4	**Maintain compliance to information security policies, regulations and standards and address risk issues** PC1. Communicate the compliance audit and risk assessment results to specified organizational personnel. PC2. Share compliance issues identified during theaudit with appropriate organizational personnel as per process laid out. PC3. Plan and coordinate the operational activities of a given company or organization to guarantee compliance with governmental regulations and ordinances. PC4. Ensure that all policies and procedures are implemented and well documented. PC5. Perform occasional internal reviews, and identify compliance problems that call for formalattention. PC6. File compliance reports with regulatory bodies. PC7. Take necessary actions for closure of the risk and non-conformance issues during the lifecycle. PC8. Present compliance issues identified to the management for prioritizing, support risk mitigation plan. PC9. Co-ordinate for ongoing monitoring of the risk factors to organizational operations and assets, individuals, other organizations. PC10. Undertake corrective actions or implementation of controls or procedural steps	25

	for satisfying needs of compliances. PC11. Implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service. PC12. Maintain quality service by establishing and enforcing organization standards. PC13. Maintain legal and regulatory compliance by researching and communicating requirements, and obtain approvals. PC14. Maintain regular communication and contact with organizational head and other departments to share information and to ensure that compliance related activities are coordinated. PC15. Document steps undertaken during the process and outcomes of the steps taken. PC16. Ensure that existing compliance related processes and procedures are being followed, with sufficient documentary evidence being maintained in the event of an internal/external audit. PC17. Complete research assignments and delivercomprehensive but concise reports in a timely manner. PC18. Provide timely feedback on contracts and agreements to be issued or entered into by the organization. PC19. Maintain professional and technical knowledge by formal and informal means. PC20. Ensure that customer needs are met within SLA and meet other time and quality commitment KPIs. PC21. Provide guidance and suggestions as appropriate. PC22. Complete own assigned tasks and activities to defined standards and timelines. PC23. Correctly follow and apply the policies and standards relating to information security identity and access management activities.	
5	**Drive interrelated cyber security actions** PC1. Identify the business functions, and key stakeholders within these, and establish their interest and understanding, relevant to achieving the organization's aims. PC2. Recognize the roles, responsibilities, interests and concerns of the stakeholders in other business functions. PC3. Identify all the activities, functions and operations that are attributed to security or require analysis from security perspective. PC4. Create an inventory of roles that are responsible, accountable and informed for activities, functions and operations in cyber security. PC5. Create an inventory of cyber security operations that fall into various key cyber security activities. PC6.Identify functions that have a joint working relationship with own function. PC7. Consider implication of own work on other functions. PC8. Discuss and consult with stakeholders from other functions in relation to key decisions and activities impacting them. PC9. Take agreements and track actionable of other functions for interrelated work. PC10. Follow up with appropriate personnel for meeting timelines and effective functioning. PC11. Agree on communication and documentation process with stakeholders and maintain the same. PC12. Identify and sort out conflicts of interest and disagreements with stakeholders, in	25

	ways that minimize damage to work and activities and to the individuals involved and the organization. PC13. Monitor and review the effectiveness of working relationships with stakeholders in other business functions, seeking and providing feedback, in order to identify areas for improvement. PC14. Fulfil agreements made with colleagues and stakeholders and let them know, advising them promptly of any difficulties, or where it will be impossible to fulfil agreements. PC15. Undertake actions agreed with stakeholders in line with the terms of any agreements made. PC16. Advise stakeholders of difficulties or where it will be impossible to fulfil agreed actions in line with the terms of any agreements made.	
6	**Manage a project team** PC1. Ensure the allocation and authorization of work to the project management team is consistent with achieving the project objectives. PC2. Brief team members on the project and their work allocations. PC3. Inform team members of changes to work allocations in an appropriate way. PC4. Provide appropriate support and guidance to team members. PC5. Monitor and assess the performance of the team against agreed objectives and work plans. PC6. Provide feedback to the team at appropriate times and locations, and in a form and manner most likely to maintain and improve their performance. PC7. Take effective action to manage any actual or potential conflict between team members. PC8. Update objectives and work plans regularly, totake account of any individual, team and organizational changes.	5
7	**Manage your work to meet requirements** 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	5
8	**Work effectively with colleagues** 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 PC9. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time	5

9	**Maintain a healthy, safe and secure working environment** 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	5
10	**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 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 PC9. provide complete, accurate and up-to-date data/information to the appropriate people in the required formats on time	5
11	**Develop your knowledge, skills and competence** PC1. obtain advice and guidance from appropriate people to develop your knowledge, skills and competence PC2. identify accurately the knowledge and skills you need for your job role PC3. identify accurately your current level of knowledge, skills and competence and any learning and development needs PC4. agree with appropriate people a plan of learning and development activities to address your learning needs PC5. undertake learning and development activities in line with your plan PC6. apply your new knowledge and skills in the workplace, under supervision PC7. obtain feedback from appropriate people on your knowledge and skills and how effectively you apply them PC8. review your knowledge, skills and competence regularly and take appropriate action	5
	Total	**200**

Reference:

1. https://nsdcindia.org/sites/default/files/MC_SSCQ0917_V1.0_Consultant%20Network%20Security_14.01.2019.pdf