GUJARAT TECHNOLOGICAL UNIVERSITY
Bachelor of Vocation (B.Voc)
Semester: III
Branch: Software Development
Subject Name: Security Analyst
Subject Code: 21130209

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory		Practical		
L	T	P	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
-	-	15	15	-	-	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	**Contribute to managing information security** PC1. establish your role and responsibilities in contributing to managing information security PC2. monitor systems and apply controls in line with information security policies, procedures and guidelines PC3. carry out security assessment of information security systems using automated tools PC4. carry out configuration reviews of information security systems using automated tools, where required PC5. carry out backups of security devices and applications in line with information security policies, procedures and guidelines, where required PC6. maintain accurate daily records/logs of information security performance parameters using standard templates and tools PC7. analyze information security performance metrics to highlight variances and issues for action by appropriate people PC8. provide inputs to root cause analysis and the resolution of information security issues, where required PC9. update your organization's knowledge base promptly and accurately with information security issues and their resolution PC10. obtain advice and guidance on information security issues from appropriate people, where required PC11. comply with your organization's policies, standards, procedures and guidelines when contributing to managing information security	40
2	**Co-ordinate responses to information security incidents** PC1. establish your role and responsibilities in co-ordinating responses to information security incidents PC2. record, classify and prioritize information security incidents using standard templates and tools PC3. access your organization's knowledge base for information on previous information security incidents and how these were managed PC4. assign information security incidents promptly to appropriate people for investigation/action PC5. liaise with stakeholders to gather, validate and provide information related to information security incidents, where required PC6. track progress of investigations into information security incidents and escalate to	40

GUJARAT TECHNOLOGICAL UNIVERSITY
Bachelor of Vocation (B.Voc)
Semester: III
Branch: Software Development
Subject Name: Security Analyst
Subject Code: 21130209

	appropriate people where progress does not comply with standards or service level agreements (SLAs) PC7. prepare accurate preliminary reports on information security incidents using standard templates and tools PC8. submit preliminary reports promptly to appropriate people for action PC9. update the status of information security incidents following investigation/action using standard templates and tools PC10. obtain advice and guidance on co-ordinating information security incidents from appropriate people, where required PC11. update your organization's knowledge base promptly and accurately with information security incidents and how they were managed PC12. comply with your organization's policies, standards, procedures, guidelines and service level agreements (SLAs) when co-ordinating responses to information security incidents	
3	**Install, configure and troubleshoot information security devices** PC1. identify the information security devices you are required to install/ configure/troubleshoot and source relevant instructions and guidelines PC2. identify any issues with instructions and guidelines for installing/configuring information security devices and clarify these with appropriate people PC3. liaise with stakeholders clearly and promptly regarding the installation/ configuration of information security devices PC4. install/configure information security devices as per instructions and guidelines PC5. test installed/configured information security devices, following instructions and guidelines PC6. resolve problems with security devices, following instructions and guidelines PC7. obtain advice and guidance on installing/configuring/testing/troubleshooting information security devices from appropriate people, where required PC8. record the installation/configuration/testing/troubleshooting of information security devices promptly using standard templates and tools PC9. provide reports for troubleshooting, configurations and deployment using standard templates and tools PC10. comply with your organization's policies, standards, procedures, guidelines and service level agreements (SLAs) when installing/configuring/troubleshooting information security devices**.**	40
4	**Contribute to information security audits** PC1. establish the nature and scope of information security audits and your role and responsibilities within them PC2. identify the procedures/guidelines/checklists for the audit tasks you are required to carry out PC3. identify any issues with procedures/guidelines/checklists for carrying out audit tasks and clarify these with appropriate people PC4. collate information, evidence and artifacts when carrying out audits PC5. carry out required audit tasks using standard tools and following established procedures/guidelines/checklists PC6. refer to appropriate people where audit tasks are beyond your levels of knowledge, skills and competence PC7. record and document audit tasks and audit results using standard tools and templates PC8. review results of audit tasks with appropriate people and incorporate their inputs	20

GUJARAT TECHNOLOGICAL UNIVERSITY
Bachelor of Vocation (B.Voc)
Semester: III
Branch: Software Development
Subject Name: Security Analyst
Subject Code: 21130209

	PC9. comply with you organization's policies, standards, procedures, guidelines and checklists when contributing to information security audits	
5	**Support teams to prepare for and undergo information security audits** PC1. establish the nature and scope of information security audits and your role and responsibilities in preparing for them PC2. identify the procedures/guidelines/checklists that will be used for information security audits PC3. identify the requirements of information security audits and prepare for audits in advance PC4. liaise with appropriate people to gather data/information required for information security audits PC5. organize data/information required for information security audits using standard templates and tools PC6. provide immediate support to auditors to carry out audit tasks PC7. participate in audit reviews, as required PC8. comply with you organization's policies, standards, procedures, guidelines and checklists when supporting teams to prepare for and undergo information security audits	20
6	**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	10
7	**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	5
8	**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	5

GUJARAT TECHNOLOGICAL UNIVERSITY
Bachelor of Vocation (B.Voc)
Semester: III
Branch: Software Development
Subject Name: Security Analyst
Subject Code: 21130209

	the designated person PC7. complete any health and safety records legibly and accurately	
9	**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	10
10	**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	10
	Total	**200**

Course Outcomes:

Sr. No.	CO Statement	Marks % Weightage
1	Apply the concepts of managing information security and Co-ordinate responses to information security incidents.	20
2	Apply the concepts of installing, configuring, troubleshooting and testing the information security devices.	20
3	Apply security audits on information with team to manage work to meet requirements.	20
4	Work effectively with colleagues in safe and secure environments and provide the information as per standard formats.	20
5	Analyze security concepts with knowledge, skills and competence.	20

Reference:

1. https://www.nqr.gov.in/qualification-title?nid=1997