GUJARAT TECHNOLOGICAL UNIVERSITY
Syllabus for Bachelor of Vocation (B.Voc.), 6th Semester
Branch: Information Technology
Subject Name: Cloud Security Analyst
(SSC-Q8309)
Subject Code: 1160508

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 Performa 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	30	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	Detect and communicate occurrences of security threats and risks to cloud assets PC1. Gather information on previous security incidents and how were they managed by accessing the organization's knowledge base PC2. Gather information on previous security incidents and how were they managed by accessing the organization's knowledge base PC3. Perform vulnerability testing and risk analysis to identify security threats and vulnerabilities in the cloud solution PC4. Implement security controls to identify security anomalies in line with data security policies, procedures and guidelines PC5. Identify security anomalies and understand their potential impact to the organization PC6. Record, classify and prioritize security incidents using standard templates and tools PC7. Ensure anomalies and incidents related to cloud security are detected in a timely manner PC8. Perform regular review and maintenance of threat detection processes PC9. Report security threats and vulnerabilities to relevant stakeholders PC10. Develop KPIs for monitoring the security incidents and identifying the root cause PC11. Leverage analytics to predict and extrapolate attack trends ahead of their occurrence PC12. Identify requirements of audit and provide assistance in audit reviews, as required PC13. Liaise with appropriate people to gather data/information required for audits PC14. Carry out required audit tasks using standard tools and following established procedures/guidelines/checklists PC15. Report outcomes of the security audits to appropriate stakeholders	100

2	Respond to security threats and restore affected capabilities PC1. Plan timely response and wherever applicable automate responses to detected security threats PC2. Execute post-incident processes and procedures in line with security policies, procedures and guidelines PC3. Maintain and update checklist, runbooks and playbooks on security incidents PC4. Assign information security incidents promptly to appropriate people for investigation/action PC5. Track progress of investigations into information security incidents PC6. Escalate security incidents to appropriate people where progress does not comply with standards or service level agreements (SLAs) PC7. Liaise with stakeholders to gather, validate and provide information 6 2 4 Qualifications Pack for Cloud Security Analyst 42 related to information security incidents, where required PC8. Report to law enforcement agencies, if required PC9. Prepare and submit accurate reports on information security incidents using standard templates and tools PC10. Prevent further expansion of the security incident PC11. Carry out backups of security devices and applications in line with security policies, procedures and guidelines, when required PC12. Ensure timely restoration of cloud assets and systems affected by security incidents PC13. Update the organization's knowledge base promptly and accurately with information security incidents and how they were managed	100
	Total	**200**

Course Outcomes

Sr.No.	Co statements:
CO 1	Gather information on previous security incidents and how were they managed by accessing the organization's knowledge base
CO 2	• Adherence to security policies and standards • Escalation and reporting of security incidents Element • Recovery & restoration of affected systems

Reference

https://nsdcindia.org/sites/default/files/SSCQ8309_Cloud_Security_Analyst_v1_20_09-2019.pdf