VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering
&
School of Information Technology and Engineering

Fall Semester 2023-24 UG Seniors (B.Tech 2021 Batch)

Continuous Assessment Test – II

SLOT: TAA1/TAA2/TCC1/TCC2

Programme Name & Branch: B.Tech & Common to all branches of SCOPE and SITE

Course Code & Name : BCSE353E, Information Security Analysis and Audit

Exam Duration: 90 Min. **Maximum Marks: 50**

General instruction(s):

Answer all the questions

Q.N0	Question	Max. Marks
1.	Attacks like Ransomware, Cerber, Crypto locker etc. continues to disrupt the businesses around the world by making valuable business data unrecoverable. The reason for these attacks being successful is ineffective backup policy. You have taken up the role of IT manager in a leading software company dealing with sensitive customer data. Design an effective backup policy for the company you are working so that these types of attacks will not affect the continuous functioning.	10
2.	Information security policies is essential for any education environment as it is the overall guidelines for the management and are a special type of document act as business rule for protecting information and the systems which store and process. ABC University accumulates lots of data from their employees and students every day through various sources. Many are not aware / handle sensitive data properly. Develop appropriate information security policy for secure information management.	10
3.	There has been a recent online breach of system security in a Government organization. The stolen information like Aadhar, mobile number and email was leaked online. As a system administrator with the organization you have been tasked with implementing information security and risk assessment process within organization. Please enumerate the risk management process to manage and mitigate the risk from the given situation.	10
4.	Companies are regularly attacked by cybercriminals and often suffer long-term damage. With increasing frequency. We live in turbulent, constantly changing times. The world is networked and digitalization is advancing. In particular, when more and more people moved their workplace to a home office. They moved	10

	from a network managed by IT professionals to a workplace with no corporate firewalls and possibly no professional antivirus programs protecting them. In this situation list the importance of security incident management?	
5.	When incident response to be successful and how teams should take a coordinated and organized approach to any incident. Mention five important steps that every response should cover in order to effectively address the wide range of security incidents that a company could experience. How to plan your incident response strategy before you need it?	10