Question Format & QP Setter Information

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name of Examination | | **Continuous Assessment Test** II (CAT), **FALL Semester- 2021** | | | | |
| **Slot: F2** | | Course Mode: CBL | | | **Class Number (s):** VL2021220103878 | |
| Course Code: | CSE3501 | | Course Title: | Information Security Analysis and Audit | | |
| Emp. No.: | 12385 | | Faculty Name: | Sendhil Kumar K.S | | School: SCOPE |
| Contact No.: | 9840068152 | | Email: | [Sendhilkumar.ks@vit.ac.in](mailto:Sendhilkumar.ks@vit.ac.in) | | |

*General Instructions (if any):****1. OPEN BOOK Examinations, 2. ….***

|  |  |
| --- | --- |
| **Q. No.** | **Question Text** |
| 1. a | What is security Assessment? Discuss in detail about various types of security assessment. Elaborate the comparative relationship between security Assessment, Analysis and Audit.  Security assessment   * + - identifies existing IT vulnerabilities (weakness) and     - recommends countermeasures for mitigating potential risks * Non-Intrusive   + Security Audit   + Risk Assessment   + Risk Analysis * Intrusive   + Vulnerability Scan   + Penetration Testing / Ethical Hacking  |  |  |  |  | | --- | --- | --- | --- | |  | **Assessment** | **Analysis** | **Audit** | | Objective | Baseline | Determine Exposure and Potential Loss | Measure against a Standard | | Method | Various (including use of tools) | Various (including tools) | Audit Program/ Checklist | | Deliverables | Gaps and Recommendations | Identification of Assets, Threats & Vulnerabilities | Audit Report | | Performed by: | Internal or External | Internal or External | Auditors | | Value | Focused Improvement | Preparation for Assessment | Compliance | |
|  | **(OR)** |
| b | Assume yourself as a owner of largest grocery shop. You have decided to sell your products in an online store to attract more customers. You have decided to develop a website for your grocery shop where customers can book the order and make payment in online itself. Give an overview of risk involved in managing the website and discuss in detail about various risk analysis tools and their usage in various modules of shopping website.  Discuss about risk involved in managing the website   * + Asset Inventory   + Software Usage   + Vulnerability Assessment   + Configuration Validation   + Penetration Testing   + Password Auditing   + Documentation |
| 1. a | Explicate your answer on why standards are important, why these standards have credibility and legitimacy. Think about what is the composition of the standard setting body and who are their members or patrons.  Security standards can help you minimize risk, reduce insurance premiums and stay on the right side of the law,  **What is a standard?**  why these standards have credibility and legitimacy  It’s simply a document written by subject experts which distils and codifies best practice. Standards have been written covering pretty much everything you can think of – from how to test forged steel eyebolts to the ethical hazards of robotics. Along the way a large number of standards have been written on security issues. These standards – written with the help of security professionals and experts from a number of industry perspectives – are a way for everyone in the sector to check and prove they are doing things in the best way possible. Security standards cover three broad areas: electronic security products, security management systems and security services. |
|  | **(OR)** |
| b | Assume yourself as a CEO of ABC software solutions. You along with other Advisory committee members develop a set of standards for your organization and ask your employees to follow those standards. Male a clear plan for advocacy and promotion of these standards to your employees so that more and more employees adopt them. List down key imperatives and challenges for the successful adoption and recognition of their proposed standards.  COBIT  ITIL  ISO  IEEE  ANSI  JTC |
| 1. a | Assume an intruder who does not belong to your organization entered into your network and modified /deleted confidential information. Your role as the Security Administrator is to help your organization understand the effectiveness of security policies and procedures across the enterprise.  You will report your effectiveness findings to Senior Management after your analysis has been completed. Prepare a detailed report and action plan for accomplish the above said task.  Understand the effectiveness of security policies and procedures across the enterprise and prepare a report on your findings. |
|  | **(OR)** |
| b | You are appointed as a Head of Security Response incident Team. Your job role is whenever a critical incident happens and affects your business operations, you have to predict and handle what comes next that will make all the difference to the extent of damage occurs to your organization. You along with your Team members. Prepare an Incident Response Action plan in order to prevent and recover your organization from damages caused by the Incident  Prepare Incident Response Action Plan for any particular incident. |

**Signature with date**