| | |
|---|---|
| **Name:**<br><br>**Enrolment No:** |  |

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**
**End Semester Examination, May,2019**

**Course: Information Security Audit and Monitoring** **Semester: XII**
**Programme: B.Tech.LL.B. CS+CL** **CC: LLBL666**
**Time: 03 hrs.** **Max. Marks: 100**
**Instructions: Attempt all questions**

**SECTION A**

| | | Marks | CO |
|---|---|---|---|
| | Write Short Notes on the followings | | |
| 1. | Governance Risk and Compliance | **2** | **CO1** |
| 2. | Information Security Best Practice | **2** | **CO 1** |
| 3. | Importance of Auditing | **2** | **CO 5** |
| 4. | ISO 27001 | **2** | **CO 4** |
| 5. | Information Technology Data Security | **2** | **CO 1** |
| | **SECTION B** | | |
| | Answer all questions | | |
| 6. | An Information security audit is a systematic, measurable technical assessment of how the organization's security policy is employed. It is part of the on-going process of defining and maintaining effective security policies. In the light of the above statement give a brief description about the basic principles of auditing. | **10** | **CO 3** |
| 7. | Information is always under threat, The heart of a cyber risk management program is an ongoing process of risk management. Explain what is ISRM and also state the importance of ISRM- Information security Risk Management Process. | **10** | **CO 5** |
| | **SECTION-C** | | |
| | Answer all questions | | |
| 8. | With ISO 27001 you can demonstrate commitment and compliance to global best practice, proving to customers, suppliers and stakeholders that security is paramount to the way you operate. State the features of the ISO 27001 standards and mentioning some of the basic standards analyze its benefits. | **10** | **CO 4** |
| 9. | Analyze the role of the government of India in ensuring Cyber security through the National Cyber Security Policy Strategies. Mention some of the important strategies and critically analyze them. | **10** | **CO 2** |

| SECTION-D | | | |
|---|---|---|---|
| | Answer all Questions | | |
| 10. | Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country.<br>You are required to draft a Cyber Security Policy for your country mentioning the followings:<br>• Name of the policy<br>• Preamble<br>• Mission and vison of the policy<br>• Regulatory Framework | **25** | **CO 5** |
| 11. | On the basis of the following circumstances mention if any offence has been committed with relevant section of IT Act 2000, also mention the penalty:<br>A. If any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract.<br>B. If a person publishes or transmits images containing a sexual explicit act or conduct.<br>C. If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.<br>D. A person fraudulently uses the password, digital signature or other unique identification of another person.<br>E. If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force. | **25** | **CO 2** |

| | |
|---|---|
| **Name:**<br>**Enrolment No:** | UPES |

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**
**End Semester Examination, May,2019**

**Course: Information Security Audit and Monitoring** **Semester: XII**
**Programme: B.Tech.LL.B. CS+CL** **CC: LLBL666**
**Time: 03 hrs.** **Max. Marks: 100**
**Instructions: Attempt all questions**

**SECTION A**

| S. No. | | Marks | CO |
|---|---|---|---|
| | Write Short Notes on the followings | | |
| 1. | What do you understand by Risk Management in GRC? | **2** | **CO1** |
| 2. | What is meant by fair dealing? | **2** | **CO 1** |
| 3. | What is the Importance of information Security monitoring | **2** | **CO 5** |
| 4. | Name any 4 documents to be created during implementation of ISO 27001:2013. | **2** | **CO 4** |
| 5. | Who should comply with PCI DSS? | **2** | **CO 1** |
| | **SECTION B** | | |
| | Answer all questions | | |
| 6. | What do you understand by Non Conformity? What is minor and major non-conformity? Give some examples. | **10** | **CO 3** |
| 7. | Explain the office of the Chief Information Security Officer (CISO). Explain his qualifications, roles and responsibilities. | **10** | **CO 5** |
| | **SECTION-C** | | |
| | Answer all questions | | |
| 8. | State the features of the ISO 27001 standards and mentioning some of the basic standards analyze its benefits and its role in Risk Assessment, Risk Treatment and creation of Risk Register for the ISO 27001:2013 Implementation. | **10** | **CO 4** |
| 9. | Critically analyze the scheme- “Cyber Surakshit Bharat”. Mentions its characteristics, features and role in enhancing the cyber security of the country. | **10** | **CO 2** |
| | **SECTION-D** | | |
| | Answer all Questions | | |

| | | | |
|---|---|---|---|
| 10. | Consider a company called YOY InfoTech Ltd, which is situated in Pune. YOY is a small company, which started 5 years back and now have 55 employees. YOY develops software for clients. YOY specializes in developing financial applications. The 60 employee comprises of 10 Java Developers (7 Software Engineer and 3 Senior Software Engineer), 10 PHP Developers (7 Software Engineer and 3 Senior Software Engineer), 5 Database Experts, 10 Testers (7 Software Engineer and 3 Senior Software Engineer), 5 Project Managers, 5 Business Developers, 5 Office Boys, 5 Network Engineer and Server Administrators, 3 HR, 1 CTO, 1 CEO.<br>All employees except office boys have been given laptops, which they can carry home as well. All employees have administrative rights to the laptops. All of them use GMAIL service for mail transfer and sometimes pen drives as well. For code repository, they use one Dropbox account, which is shared by all the employees.<br>Their office is completely WIFI based and whenever there is any client visit, the client also uses the same WIFI, even the office boys also uses same WIFI to use internet on their mobiles. Office boys help in Xerox, printouts, files transfer, courier etc.<br>You are a Consultant working for EWC and YoY has given you a project namely:<br>Risk Assessment, Risk Treatment and creation of Risk Register for their ISO 27001:2013 Implementation. | **25** | **CO 5** |
| 11. | YoY has asked for an initial kickoff meeting with EWC regarding implementation of PCI DSS and required clarity on the following:<br>a) How to do segmentation?<br>b) Components to be involved in Penetration testing<br>Being a consultant from EWC, you will be giving presentation during this meeting, so prepare short notes for both a and b**.** | **25** | **CO 2** |