# CONFIDENTIAL

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Name of Examination** (Please tick, symbol is given) | : | **MID** | | **END** | ✓ | **SUPPLE** | |
| **Name of the College** (Please tick, symbol is given) | : | **COES** | | **CMES** | | **COLS** | ✓ |
| **Program/Course** | : | Int. B.Tech + LLB (Cyber Law) | | | | | |
| **Semester** | : | **12** | | | | | |
| **Name of the Subject** | : | **Information Security Audit & Monitoring** | | | | | |
| **Subject Code** | : | **LLBL666** | | | | | |
| **Name of Question Paper Setter** | : | **Jatin Sethi** | | | | | |
| **Employee Code** | : | **40001283** | | | | | |
| **Mobile & Extension** | : | **887861678** | | | | | |
| **Note: Please mention additional Stationery to be provided, during examination such as Table/Graph Sheet etc. else mention "NOT APPLICABLE":**<br><br>**Not Applicable** | | | | | | | |

FOR SRE DEPARTMENT

| | | |
|---|---|---|
| Date of Examination | : | |
| Time of Examination | : | |
| No. of Copies (for Print) | : | |

**Note: - Pl. start your question paper from next page**

**Roll No: ----------**

# UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

**End Semester Examination, April 2017**

**Program Name:** Int. B.Tech + LLB (Cyber Law) **Semester – 12**
**Course Name :** Information Security Audit & Monitoring **Max. Marks : 100**
**Course Code :** LLBL666 **Duration : 3 Hrs**
**No. of page/s:** 03

**Note:**

1. Answers to question 1 to 5 of Section A carries 4 marks each.
2. Answers to question 6 to 9 of Section B carries 10 marks each.
3. Answers to question 10 and 11 of Section C carries 20 marks each.
4. Please answer specifically and precisely.

## SECTION A

1. Name all the principles of COBIT 5.

2. What do you understand by Risk Management in GRC?

3. Explain the functioning of COBIT 5 cascade using block diagram only.

4. Name any 8 documents to be created during implementation of ISO 27001:2013.

5. Who should comply with PCI DSS?

## SECTION B

6. (a) What is HIPAA?
(b) Who must comply with HIPAA?
(c) What is PHI as per HIPAA?

7. Complete the following table related to activities involved in Audit (First row has been done as an example):

| Activity Order | Activity | Activity Insights (only mention pointwise) |
|---|---|---|
| Activity 1 | Scoping & Pre Audit Survey | • Identify Information Sources<br>• Identify Business Units to be in scope<br>• Meeting with the stakeholders<br>• Allocation of Audit Escorts |

| | | |
|---|---|---|
| Activity 2 | ? | ? |
| Activity 3 | ? | ? |
| Activity 4 | ? | ? |
| Activity 5 | ? | ? |
| Activity 6 | ? | ? |

8. What do you understand by Non Conformity? What is minor and major non-conformity? Give some examples.

9. Map the following offences with relevant section of IT Act 2000, also mention the penalty:

| S.No. | Offence | Section | Penalty |
|---|---|---|---|
| 1 | 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 | | |
| 2 | If a person publishes or transmits images containing a sexual explicit act or conduct. | | |
| 3 | If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge. | | |
| 4 | A person fradulently uses the password, digital signature or other unique identification of another person. | | |
| 5 | 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. | | |

## SECTION C

**(Note: Please use the case study given below, for question 10 & 11)**

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.

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.
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.

You are a Consultant working for EWC and YoY has given you two projects namely

i. Implementation of PCI DSS

ii. Risk Assessment, Risk Treatment and creation of Risk Register for their ISO 27001:2013 Implementation

**10**. YoY has asked for an initial kickoff meeting with EWC regarding implementation of PCI DSS and required clarity on the following:

a) How to do segmentation?
b) Components to be involved in Penetration testing
c) Difference between QSAC & ASV
d) Difference between PCI DSS & PA DSS

Being a consultant from EWC, you will be giving presentation during this meeting, so prepare short notes for both a and b.

**11.**
(a) Perform Risk Assessment using the generic approach and create a risk register with at least 10 risk.

**OR**

(b) Perform Risk Assessment using the FAIR Model and create a risk register with at least 10 risk.

**Roll No: ----------**

# UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

**End Semester Examination, April 2017**

**Program Name:** Int. B.Tech + LLB (Cyber Law) **Semester – 12**
**Course Name :** Information Security Audit & Monitoring **Max. Marks : 100**
**Course Code :** LLBL666 **Duration : 3 Hrs**
**No. of page/s:** 03

**Note:**

1. Answers to question 1 to 5 of Section A carries 4 marks each.
2. Answers to question 6 to 9 of Section B carries 10 marks each.
3. Answers to question 10 and 11 of Section C carries 20 marks each.
4. Please answer specifically and precisely.

## SECTION A

1. Name all the enablers of COBIT 5.

2. What do you understand by Compliance in GRC?

3. Explain the functioning of COBIT 5 cascade using block diagram only.

4. Name any 8 documents to be created during implementation of ISO 27001:2013.

5. What is open payment system and closed payment system as per PCI DSS?

## SECTION B

6. (a) What is SOX?
(b) Who must comply with SOX?
(c) Which sections of SOX are related to information security?

7. Complete the following table related to activities involved in Audit (First row has been done as an example):

| Activity Order | Activity | Activity Insights (only mention pointwise) |
|---|---|---|
| Activity 1 | Scoping & Pre Audit Survey | • Identify Information Sources<br>• Identify Business Units to be in scope<br>• Meeting with the stakeholders<br>• Allocation of Audit Escorts |

| | | |
|---|---|---|
| Activity 2 | ? | ? |
| Activity 3 | ? | ? |
| Activity 4 | ? | ? |
| Activity 5 | ? | ? |
| Activity 6 | ? | ? |

8. What do you understand by audit trails? How audit trails can lead to non-conformities.

9. Map the following offences with relevant section of IT Act 2000, also mention the penalty:

| S.No. | Offence | Section | Penalty |
|---|---|---|---|
| 1 | If any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person | | |
| 2 | If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18. | | |
| 3 | If a person cheats someone using a computer resource or communication. | | |
| 4 | A person receives or retains a computer resource or communication device, which is known to be stolen, or the person has reason to believe is stolen. | | |
| 5 | 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. | | |

## SECTION C

**(Note: Please use the case study given below, for question 10 & 11)**

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.
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.
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.

You are a Consultant working for EWC.

**10**. Create a proposal for YoY that they should implement ISO 27001 and should go for Certification where your firm EWC will help them for implementation. Your proposal may have maximum of 5 slides. (Note: One Slide = One heading or 2 subheadings for exam purpose).

**11**. YoY is also going for implementation of PCI DSS, but have some doubts mentioned, if you may clear the doubts, YoY will probably will give this project to your EWC also:

**(a)** What is the difference between PA DSS and PCI DSS? How to comply with PCI DSS, which are the phases? What is the difference between QSAV and ASV?

**OR**

**(b)** How to perform segmentation and how to do sampling? What is the importance of Penetration Testing in PCI DSS, which components are involved during penetration testing?