

Roll No: -----



UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, April 2018

Program: B.Tech. (Computer Science & Engineering), LL.B. (Hons.) in Cyber Law

Semester – **XII**

Subject (Course): Information Security Audit and Monitoring

Max. Marks: 100

Course Code: LLBL 666

Duration: 3 Hrs

No. of page/s:3

Note: All questions are compulsory.

Section A: (5*2=10)

1. Name any four GRC automation tools.
2. Write any 4 benefits of ISO 27001.
3. How Risk Acceptance is different from Risk Avoidance?
4. Name the following ISO series:
 - a. ISO 27002
 - b. ISO 27003
5. What is PCI DSS?

Section B: (2*10=20)

1. Explain the basic principles of Audit. What do you understand by first , second and third party audit?
2. Explain the PDCA cycle.

Section C: (2*10=20)

1. Why is risk management needed and how is risk assessment performed?
2. Explain the objectives of an Audit Program. Also, explain the business value of auditing.

Section D: (2*25=50)

- 1. Complete the following table related to activities involved in Audit (First row has been done as an example): (Explain all activities)**

Activity Order	Activity	Activity Insights
Activity 1	Scoping & Pre Audit Survey	<ul style="list-style-type: none">• Identify Information Sources• Identify Business Units to be in scope• Meeting with the stakeholders• Allocation of Audit Escorts
Activity 2	?	?
Activity 3	?	?
Activity 4	?	?
Activity 5	?	?
Activity 6	?	?

- 2. Consider a company called SoL InfoTech Ltd, which is situated in Dehradun. SoL is a small company, which started 5 years back and now have 60 employees. SoL develops software for clients. SoL 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 CL12. Create a proposal for SoL that they should implement ISO 27001 and should go for Certification where your firm CL12 will help them for implementation.

Roll No: -----



UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, April 2018

Program: B.Tech. (Computer Science & Engineering), LL.B. (Hons.) in Cyber Law

Semester – **XII**

Subject (Course): Information Security Audit and Monitoring

Max. Marks: 100

Course Code: LLBL 666

Duration: 3 Hrs

No. of page/s: 2

Section A: (5*2=10)

1. Name any four GRC automation tools.
2. Write any 4 benefits of ISO 27001.
3. How Risk Acceptance is different from Risk Avoidance?
4. Name the following ISO series:
 - a. ISO 27002
 - b. ISO 27003
5. What is PCI DSS?

Section B: (2*10=20)

3. Explain the basic principles of Audit. What do you understand by first , second and third party audit?
4. Explain the PDCA cycle.

Section C: (2*10=20)

3. Why is risk management needed and how is risk assessment performed?
4. Explain the objectives of an Audit Program. Also, explain the business value of auditing.

Section D: (2*25=50)

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

Activity Order	Activity	Activity Insights
Activity 1	Scoping & Pre Audit Survey	<ul style="list-style-type: none">• Identify Information Sources• Identify Business Units to be in scope• Meeting with the stakeholders• Allocation of Audit Escorts
Activity 2	?	?
Activity 3	?	?

Activity 4	?	?
Activity 5	?	?
Activity 6	?	?

4. Consider a company called SoL InfoTech Ltd, which is situated in Dehradun. SoL is a small company, which started 5 years back and now have 60 employees. SoL develops software for clients. SoL 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 CL12. Create a proposal for SoL that they should implement ISO 27001 and should go for Certification where your firm CL12 will help them for implementation.