

Name:

Enrolment No:



**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**End Semester Examination, May 2019**

**Course: Information Systems – Risk & Security**

**Programme: BBA Accounting Information Systems**

**Time: 03 Hours**

**Instructions: Please answer the questions strictly in Context**

**Semester: IV**

**C. Code: STGM 2001**

**Max. Marks: 100**

**SECTION A**

**Write on the following in brief**

**Marks**

**CO**

Q.1.	Firewall	3	1
Q.2.	Integrity	3	1
Q.3.	Availability	3	1
Q.4.	Control	3	1
Q.5.	Cost-Benefit Analysis	3	5
Q.6.	Phishing	3	1
Q.7.	Trojan	3	1
Q.8.	Keylogger	3	1
Q.9.	SLE	4	5
Q.10.	Click Fraud	4	5
Q.11.	Denial of Service (DoS) Attacks	4	5
Q.12.	SQL Injection Attacks	4	5
Q.13.	SSL	5	5
Q.14.	Sarbanes-Oxley Act.	5	5

**SECTION B**

**Attempt all Questions**

**Marks**

**CO**

Q.1.	Describe the various 'Security Risk Management Maturity Levels' of organizations with examples	10	1
Q.2.	What are the tools and methods used for Identity Management and Authentication ?	10	1
Q.3.	Discuss in detail the controls we need to have in place to protect our Information Systems.	10	3

**SECTION C**

**Attempt this section**

**Marks**

**CO**

Q.1.	How are Business Continuity Planning and Disaster Recovery planning helpful for a Business? Furnish cases in brief.	20	4
------	---	----	---

Name:

Enrolment No:



**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**End Semester Examination, May 2019**

**Course: Information Systems – Risk & Security**

**Programme: BBA Accounting Information Systems**

**Time: 03 Hours**

**Instructions: Please answer the questions strictly in Context**

**Semester: IV**

**C. Code: STGM 2001**

**Max. Marks: 100**

**SECTION A**

**Write on the following in brief**

		<b>Marks</b>	<b>CO</b>
Q.1.	Asset	<b>3</b>	<b>1</b>
Q.2.	Integrity	<b>3</b>	<b>1</b>
Q.3.	Availability	<b>3</b>	<b>1</b>
Q.4.	Control	<b>3</b>	<b>1</b>
Q.5.	Cost-Benefit Analysis	<b>3</b>	<b>5</b>
Q.6.	Impact	<b>3</b>	<b>1</b>
Q.7.	Mitigation	<b>3</b>	<b>1</b>
Q.8.	Risk	<b>3</b>	<b>1</b>
Q.9.	Denial of Service (DoS)Attacks	<b>4</b>	<b>5</b>
Q.10.	SQL Injection Attacks	<b>4</b>	<b>5</b>
Q.11.	Click Fraud	<b>4</b>	<b>5</b>
Q.12.	SLE	<b>4</b>	<b>5</b>
Q.13.	SSL	<b>5</b>	<b>4</b>
Q.14.	SOX	<b>5</b>	<b>4</b>

**SECTION B**

**Attempt all Questions**

		<b>Marks</b>	<b>CO</b>
Q.1.	Elaborate the four phases of the ‘Security Risk Management Process’.	<b>10</b>	<b>1</b>
Q.2.	What are the tools and methods used for Identity Management and Authentication?	<b>10</b>	<b>3</b>
Q.3.	Discuss in detail the controls we need to have in place to protect our Information Systems.	<b>10</b>	<b>3</b>

**SECTION C**

**Attempt this section**

		<b>Marks</b>	<b>CO</b>
Q.1.	Describe the various ‘Security Risk Management Maturity Levels’ of organizations with examples	<b>20</b>	<b>4</b>