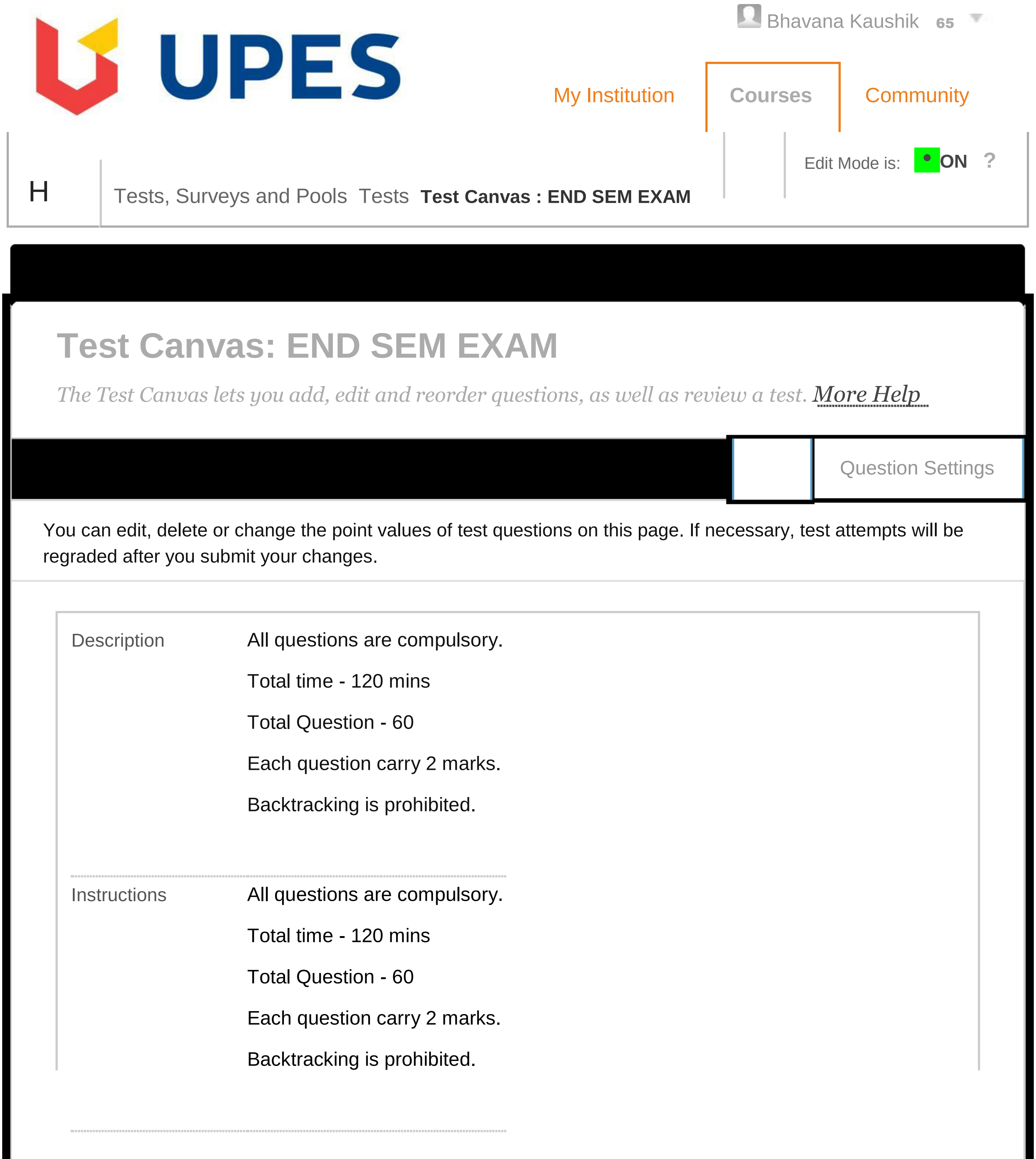
Name: **Enrolment No:**	UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2020

Course: Information Security Audit and Monitoring **Semester: VI**
Course Code: CSSF 3004
Time: 10 AM-1 PM
Programme: BTECH CSE +CSF **Max. Marks: 100**
Instructions: Attempt all questions

/30/2020 Test Canvas: END SEM EXAM – Information Security Audit &...



Test Canvas: END SEM EXAM

The Test Canvas lets you add, edit and reorder questions, as well as review a test. More Help

You can edit, delete or change the point values of test questions on this page. If necessary, test attempts will be regraded after you submit your changes.

Description	All questions are compulsory. Total time - 120 mins Total Question - 60 Each question carry 2 marks. Backtracking is prohibited.
Instructions	All questions are compulsory. Total time - 120 mins Total Question - 60 Each question carry 2 marks. Backtracking is prohibited.

Total Questions	60
Total Points	120
Number of Attempts	149

Select: All None Select by Type: - Question Type -

Delete and Regrade Points □ Update and Regrade Hide Question Details

1. Multiple Choice: According to the section "context of ...

Points: 2

Question

According to the section "context of the organization" of ISO/IEC 27001, which of the following activities are required?

a) Determine the requirements of interested parties relevant to information security

b) Establish organizational responsibilities for suppliers in collaboration with administrative units

c) Determine the interested parties that are relevant to the ISMS

Answer

✓ only c

a and c

b and c

a, b and c

□ 2. Multiple Choice: GRC Risk Management is used to m...

Points: 2

Question GRC Risk Management is used to manage and control all types of risks occurring or going to occur in the future. Which of the following is true regarding it?

Answer

It also comprises of various solutions to risks.

It identifies risks in an organization.

perform qualitative and quantitative analysis of risks to figure out the level of risk to decide for the organization whether to take it or not

✓ all of the above

□ 3. True / False: "The audit planning strategies are de...

Points: 2

Question "The audit planning strategies are defined by audit entities and these can be linked to Process control and Risk management to find risks, controls, etc."

Answer

✓ True

False

□ 4. Multiple Choice: The role of internal auditors: ...

Points: 2

Question

The role of internal auditors:

A)Performing risk assessment on a regular basis

B) Providing specific requirements for audit purpose

C) They act as a liaison between external auditors.

Answer

A and B

✓ A, B and C

B and C

A and C

□ 5. Fill in the Blank: What does O stands for in COBIT

Points: 2

Question	What does O stands for in COBIT	
Evaluation Method	**Answer**	**Case Sensitivity**
Exact Match	objectives	

□ 6. Fill in the Blank: Year of development of COBIT 5

Points: 2

Question	Year of development of COBIT 5	
Evaluation Method	**Answer**	**Case Sensitivity**
Exact Match	2012	

□ 7. Multiple Choice: Who uses COBIT: a) Owners of the proc...

Points: 2

Question Who uses COBIT: a) Owners of the process b) the risk committees c)Managers and Directors of IT - choose the correct anwer

Answer

a and b

a and c

b and c

✓ "a, b and c"

Points: 2

□ 8. Multiple Choice: A) Governance looks after the perspec...

Question A) Governance looks after the perspectives and laws which are required in the organization. B) Compliance is the measures taken up by the company to follow to governance in various manners.

Answer

✓ Both A and B are correct

only A is correct

only B is correct

None of them is correct

Points: 2

□ 9. True / False: COBIT 5 brings together the five prin...

Question COBIT 5 brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders.

Answer

✓ True

False

Points: 2

□ 10. True / False: COBIT is designed to help enterprises...

Question COBIT is designed to help enterprises to Keep IT-related risk at an acceptable level and Optimize IT services and technology costs.

Answer

✓ True

False

Points: 2

□ 11. Multiple Choice: Which of the followings are enablers ...

Question Which of the followings are enablers for business- information security alignment

Answer

Hierarchy

✓ competencies

government

none

Points: 2

□ 12. **Multiple Choice: It was formed in the year of 1969 and...**

Question	It was formed in the year of 1969 and it was run by a small circle of individuals who realized that there was a need for a source of guidance and information in the then upcoming field of computer system s control of auditing.
Answer	✓ ISACA GRC COBIT NONE

Points: 2

□ 13. **Fill in the Blank: For how many years the ISO 27001:2013...**

Question	For how many years the ISO 27001:2013 certificate valid? (one word only)	
Evaluation Method	**Answer**	**Case Sensitivity**
Exact Match	three	

Points: 2

□ 14. **Matching: Match the following**

Question	Match the following		
Answer	Match Question Items		Answer Items
	A. -	A. Aim of the ISO 27001:2013	A. consistent and centrallycontrolled management system for protecting information.
	B. -	B. Benefits of ISO 27001 certification	B. protecting your organization from cyber attacks, loss of data and the resulting financial losses and damage to reputation
	C. -	C. what does ISMS means	C. systematic approach that takes into account both technical and human factors

Points: 2

□ 15. Multiple Choice: "Organizations are required to equip ...

Question "Organizations are required to equip their networks according to minimum standards. In addition, technical and organizational provisions need to be met to ensure the following"

Answer

- Availability
- Authenticity
- ✓ both
- none

Points: 2

□ 16. True / False: Only someone who s been trained and c...

Question Only someone who s been trained and certified as an ISO/IEC 27001 Lead Auditor can audit an organization for ISO/IEC 27001 compliance

Answer

- ✓ True
- False

Points: 2

□ 17. Matching: Match the following

Question Match the following

Answer

Match	Question Items	Answer Items
C. -	A. Evaluate risks	A. "risks that can affect the confidentiality, integrity and availability of information "
A. -	B. Identify risks	B. dentify the threats and vulnerabilities that apply to each asset
B. -	C. Analyse risks?	C. identify which risks are worth treating and?prioritise?them

Points: 2

□ 18. Matching: Match the following

Question Match the following

Answer

Match	Question Items	Answer Items
C. -	A. comments report	A. "providing an overview of the assessment, including relevant assets, the treatment applied, and the estimated impact and probability of each risk"

A. -	B. risk assessment report	B. "detailing the residual risk, i.e. the risks that remain after risk treatment"
B. -	C. risk summary report	C. "attached to your risk assessment, to explain your decisions in more detail"

□ 19. Multiple Choice: P. Establish and maintain certain inf...

Points: 2

Question

P. Establish and maintain certain information security risk criteria;

Q. Analyse and evaluate information security risks according to certain criteria.

R. Identify the owners of those risks

S. Ensure that repeated risk assessments “produce consistent, valid and comparable results”;

T. “Identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system”;

Identify the correct sequence of the above statements

Answer

✓ P-S-T-R-Q

P-T-R-S-Q

R-P-Q-S-T

P-R-Q-S-T

□ 20. Matching: Match the following

Points: 2

Question Match the following

Answer

Match	Question Items	Answer Items
D. -	A. Tolerating the risk	A. by changing your processes to stop the risky behaviour
A. -	B. Terminating the risk	B. by applying a security control to minimise the likelihood of it occurring or the impact it will have
B. -	C. Treating the risk	C. by purchasing cyber insurance or outsourcing the process
C. -	D. Transferring the risk	D. if the problem isn t serious enough to justify using resources to tackle it or the process cannot be avoided

Points: 2

□ 21. Multiple Choice: "What is the part of ""Support"" ISO ...

Question	"What is the part of ""Support"" ISO 27001:2013?"
Answer	Communication
	Competence
	Awareness
	✓ all the above

Points: 2

□ 22. True / False: "Management plans, builds, runs and m...

Question	"Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives "
Answer	✓ True False

Points: 2

□ 23. Multiple Choice: Which term is associated to clause 5 ...

Question	Which term is associated to clause 5 of ISO 27001?
Answer	✓ leadership
	support
	operation
	planning

Points: 2

□ 24. Multiple Choice: ensuring that employees can only view...

Question	ensuring that employees can only view information that s relevant to their job role.
Answer	information security policy
	operation security
	✓ access control
	asset management

Points: 2

□ **25. Multiple Choice: a) The Payment Card Industry Data Sec...**

Question a) The Payment Card Industry Data Security Standard (PCI DSS) applies to companies of any size that accept credit card payments.

b) If your company intends to accept card payment, and store, process and transmit cardholder data, you need to host your data securely with a PCI compliant hosting provider

On the basis of above statements a) and b) identify the correct choice

Answer

Only a is correct

only b is correct

✓ both are correct

none is correct

Points: 2

□ **26. Multiple Choice: Which response most accurately descri...**

Question Which response most accurately describes PCI DSS compliance?

Answer

The organization can guarantee that credit card data will never be lost.

✓ The organization has followed the rules set forth in the Payment Card Industry Data Security Standard and can offer proof in the form of documentation.

The organization is not liable if credit card data is lost or stolen.

The organization does not store PAN or CVV data under any circumstances.

Points: 2

□ **27. Multiple Choice: Which of the following Web applicatio...**

Question	Which of the following Web application security requirements is mandated by the PCI DSS?
Answer	Code reviews Checks to ensure applications are not vulnerable to the OWASP Top 10 Integration of security throughout the software development life cycle ✓ All of the above

□ **28. Multiple Choice: Which of the following can be stored ...**

Points: 2

Question	Which of the following can be stored according to the PCI DSS?
Answer	CVV/CVC ✓ PANs and cardholder names PANs and CVVs/CVCs PIN blocks

□ **29. Fill in the Blank: "Fill in the blank: In PCI DSS, an AS...**

Points: 2

Question "Fill in the blank: In PCI DSS, an ASV is an ___________ . "

Evaluation Method	Answer	Case Sensitivity
Exact Match	Approved Sanning Vendor	

□ **30. Fill in the Blank: "If an organization is using a virtua...**

Points: 2

Question "If an organization is using a virtual terminal system like PayPal, and accesses it from a computer on company premises, does the desktop computer need to be segregated or isolated from other internal systems in order to keep those other systems outside the scope of PCI DSS?

Type Yes or No!

Evaluation Method	Answer	Case Sensitivity
Exact Match	yes	

□ **31. Multiple Choice: a) PCI DSS was created by the major c...**

Points: 2

Question

a) PCI DSS was created by the major credit card companies
b) Merchants can store authentication data - i.e. full magnetic stripe data, CVV2 - but only if that information is encrypted.

Answer

✓ only a is correct

only b is correct

both are correct

none is correct

□ **32. True / False: "If a merchant is PCI Compliant, it i...**

Points: 2

Question	"If a merchant is PCI Compliant, it is impossible for a cardholder data breach to occur."
Answer	True ✓ False

□ **33. Fill in the Blank: "systematic, independent and document...**

Points: 2

Question

"systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled is called _________________"

Evaluation Method	**Answer**	**Case Sensitivity**
Exact Match	audit	

□ **34. Matching: Match the following**

Points: 2

Question Match the following

Answer

	Match Question Items	Answer Items
B. -	A. infrastructure failure	A. "someone might accidentally delete important data, or fail to follow security procedures properly."
C. -	B. Technical Failure	B. loss of your internet connection can interrupt your business - eg you could miss an important purchase order.
D. -	C.	C.

	electronic threat	you cannot retrieve data on a failed hard drive and no backup copy is available.
A. -	D. Human Error	D. "a hacker could get access to your website, your IT system could become infected by a computer virus, or you could fall victim to a fraudulent email or website."

□ **35. Fill in the Blank: how many control objectives are there...**

Points: 2

Question	how many control objectives are there in PCI-DSS(write in words)	
Evaluation Method	**Answer**	**Case Sensitivity**
Exact Match	six	

□ **36. Matching: Match the following**

Points: 2

Question	Match the following		
Answer		Match Question Items	Answer Items
	A. -	A. Protect Cardholder Data	A. "Encrypt transmission of cardholder data across open, public networks "
	B. -	B. Build and Maintain a Secure Network and Systems	B. Do not use vendor-supplied defaults for system passwords
	D. -	C. Maintain a Vulnerability Management Program	C. Track and monitor all access to network resources
	C. -	D. Regularly Monitor and Test Networks	D. Protect all systems against malware

□ **37. True / False: "While healthcare providers must foll...**

Points: 2

Question	"While healthcare providers must follow HIPAA rules, health insurance companies are not responsible for protecting patient information. "
Answer	True ✓ False

□ **38. True / False: Billing information is protected unde...**

Points: 2

Question	Billing information is protected under HIPAA
Answer	✓ True False

□ **39. Matching: Match the following**

Points: 2

Question	Match the following	
Answer	Match Question Items	Answer Items
	C.- A. Publishing information which is obscene in electronic form	A. section 66A
	A. - B. "Publishing offensive, false or threatening information"	B. section 66
	B. - C. Hacking with computer system	C. section 67
	D. - D. Failure/refusal to comply with orders	D. section 68

□ **40. Multiple Choice: Scoping and pre audit surveys of Audi...**

Points: 2

Question	Scoping and pre audit surveys of Auditing steps involve
Answer	✓ Fixing objectives
	identifying audit team
	identfying type of audit
	none of the above

□ **41. Multiple Choice: Analysis and test of Auditing steps i...**

Points: 2

Question	Analysis and test of Auditing steps involves
Answer	organization visits
	✓ audit trail analysis
	fixing objectives
	identifying audit team

□ **42. Multiple Choice: "Audits carried out by an o...**

Points: 2

Question	"Audits carried out by an organisation on its supplier (partners, vendors) using, either internal personnel, or entrusted with doing it."
Answer	first party audit
	✓ second party audit
	third party audit

none of the above

Points: 2

□ 43. **Multiple Choice: Which of the following is NOT a purpo...**

Question	Which of the following is NOT a purpose of HIPAA?
Answer	To prevent abuse of information in health insurance and healthcare.
	✓ To establish continuous healthcare coverage for patients who are switching jobs.
	To better manage protected health information.
	all of the above

Points: 2

□ 44. **Multiple Choice: What is PHI?**

Question	What is PHI?
Answer	Private HIPAA Information
	Personal Health Information
	✓ Protected Health Information
	None of the above

Points: 2

□ 45. **Multiple Choice: Which of the following is NOT example...**

Question	Which of the following is NOT example of PHI
Answer	Patient's demographic information in computer for appointment at health dept
	Patient's paper lab report that hasn't been filed yet
	✓ A report containing the number of HIV cases in the state of TN
	A nurse discussing a patient's diagnosis with a physician

Points: 2

□ 46. **Multiple Choice: Which of the following is not a requi...**

Question Which of the following is not a requirement for computer security

Answer

Computers must be password protected.

✓ Computer must be secured to desk with an anti-theft device.

"PHI can't be sent in the body of an email, has to be sent as a password-protected attachment."

Computer monitors displaying PHI must face away from the public or have a privacy screen.

□ 47. Multiple Choice: An example of a HIPAA violation and a...

Points: 2

Question An example of a HIPAA violation and a possible breach of unsecured PHI would be:

Answer

Accessing the computer to get information on a neighbor.

Releasing a copy of a record to an unauthorized recipient.

Disclosing PHI in a conversation with someone outside of the Health Dept.

✓ All of the above.

□ 48. Multiple Choice: What is HIPAA?

Points: 2

Question What is HIPAA?

Answer

The federal rules for Medicare payments.

✓ The federal standards for the protection of health information.

The federal rules for Medicaid payments

The state rules for Medicaid.

□ 49. Multiple Choice: The covered entity may use or discl...

Points: 2

Question The covered entity may use or disclose protected health information when:

Answer

✓ The individual who is subject of the information (or the individual s personal representative) authorizes in writing.

The information is requested by a family member

The information is requested by the spouse

all of the above

□ 50. True / False: ". If a patients refuses to allow the...

Points: 2

Question ". If a patients refuses to allow the agency to share his patient information with family members, the agency can refuse to provide services to this patient."

Answer

True

✓ False

□ 51. True / False: The covered entity must accept all re...

Points: 2

Question The covered entity must accept all requests by the patient for restrictions to the release of the patient information no exceptions.

Answer

True

✓ False

□ 52. Multiple Choice: Who is not covered by the Privacy Rul...

Points: 2

Question Who is not covered by the Privacy Rule as per HIPAA?

Answer

Health plans

Health providers

Business associate

✓ Family members

□ 53. Matching: Match the following

Points: 2

Question Match the following

Answer

	Match Question Items	Answer Items
D. -	A. risk criteria	A. action to eliminate a detected nonconformity
A. -	B. correction	B. action to eliminate the cause of a nonconformity and to prevent recurrence
C. -	C. risk owner	C. person or entity with the accountability and authority to manage a risk
B. -	D.	D.

corrective action	terms of reference against which the significance of risk is evaluated

□

Points: 2

54. Multiple Choice: What is/are component of IT Act 2000 ?

Question	What is/are component of IT Act 2000 ?
Answer	Legal Recognition to Digital Signatures Regulation of Certification Authorities. Digital Certificates ✓ All the above

□

Points: 2

55. Multiple Choice: Which Act in India focuses on data pr...

Question	Which Act in India focuses on data privacy and information technology?
Answer	Banking Regulation Act 1949 IT Act 2000 Indian Penal Code ✓ IT (amendment) Act 2008

□

Points: 2

56. Multiple Choice: The following punishment is mentioned...

Question	The following punishment is mentioned in which section of IT Act 2000 '3 years of imprisonment and/or 5 lakh repees penalty for first conviction & 5 years of imprisonment and/or 10 lakh rupees penalty
Answer	✓ Section 67 Section 66 Section 64 Section 65

Points: 2

□

57. Multiple Choice: Which section of IT Act deals with Cy...

Question	Which section of IT Act deals with Cyber terrorism?
Answer	Section 66C Section 66B ✓ Section 66F Section 66A

□ 58. Multiple Choice: Internal policies are related to whic...

Points: 2

Question	Internal policies are related to which component of GRC
Answer	COMPLIANCE ✓ GOVERNANCE RISK MANAGEMNT NONE

□ 59. Multiple Choice: "Which of the following statements ar...

Points: 2

Question	"Which of the following statements are correct with respect to ISO/IEC 27001, Annex A?"
Answer	✓ Annex A defines control objectives for information security. Annex A is a catalog of security threats. Risk documentation criteria none of the above

□ 60. Matching: Match the following

Points: 2

Question	Match the following	
Answer	Match Question Items	Answer Items
	B. - A. Operations security	A.

		"the agreements to include in contracts with third parties,"
C. -	B. Physical and environmental security	B. ensuring that information processing facilities are secure.
A. -	C. Supplier relationships	C. securing the organisation s premises and equipment.
D. -	D. Communications security	D. how to protect information in networks.

Select: All None Select by Type: - Question Type -

Delete and Regrade | Points □ Update and Regrade | Hide Question Details

← OK