



**Free Questions for *ISSMP* by *vceexamstest***

**Shared by *Baird* on *12-12-2023***

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

**Question Type:** MultipleChoice

---

Which of the following laws is defined as the Law of Nations or the legal norms that has developed through the customary exchanges between states over time, whether based on diplomacy or aggression?

**Options:**

---

- A- Customary
- B- Tort
- C- Criminal
- D- Administrative

**Answer:**

---

A

**Explanation:**

---

The customary law refers to the Law of Nations or the legal norms that have developed through the customary exchanges between states over time, whether based on diplomacy or aggression. The customary law is built upon the ideas of personal conduct and tradition of a country.

Essentially, legal obligations are believed to arise between states to carry out their affairs consistently with past accepted conduct. These customs can also change based on the acceptance or rejection by states of particular acts. Some principles of customary law have achieved the force of peremptory norms, which cannot be violated or altered except by a norm of comparable strength. These norms are said to gain their strength from universal acceptance, such as the prohibitions against genocide and slavery.

Answer option B is incorrect. Tort law is a body of law that deals with civil wrongdoings. The definition of this kind of wrong is usually distinct from a criminal wrong. A person who suffers legal damage may be able to use tort law to receive damages (usually monetary compensation) from someone who is responsible or liable for those injuries. Generally speaking, tort law defines what a legal injury is and what is not.

A person may be held liable (responsible to pay) for another's injury caused by them. The major categories of torts are intentional torts, negligent torts, and strict liability torts.

Answer option D is incorrect. The administrative law is the body of law that governs the activities of administrative agencies of government.

Government agency action can include rulemaking, adjudication, or the enforcement of a specific regulatory agenda. Administrative law is considered a branch of public law.

As a body of law, administrative law deals with the decision-making of administrative units of government (e.g., tribunals, boards or commissions) that are part of a national regulatory scheme in such areas as police law, international trade, manufacturing, the environment, taxation, broadcasting, immigration and transport.

Answer option C is incorrect. The criminal law, or penal law, is the body of rules with the potential for severe impositions as punishment for failure to comply. Criminal punishment, depending on the offense and jurisdiction, may include execution, loss of liberty, government supervision (parole or probation), or fines. Criminal law typically is enforced by the government, unlike the civil law, which may be enforced by private parties.

## Question 2

---

**Question Type:** MultipleChoice

---

Tomas is the project manager of the QWS Project and is worried that the project stakeholders will want to change the project scope frequently. His fear is based on the many open issues in the project and how the resolution of the issues may lead to additional project changes. On what document are Tomas and the stakeholders working in this scenario?

### Options:

---

- A- Communications management plan
- B- Change management plan
- C- Issue log
- D- Risk management plan

## Answer:

---

B

## Explanation:

---

The change management plan defines how the change control system works and the proper channels and procedures manages changes within the project. Change control system, a part of the configuration management system, is a collection of formal documented procedures that

define how project deliverables and documentation will be controlled, changed, and approved.

Answer option C is incorrect. The issue log is a document that records all issues, their characteristics, and status.

Answer option A is incorrect. The communications management plan defines who needs what information, when the information is needed, and the modality the information is to be communicated in.

Answer option D is incorrect. The risk management plan defines how risk will be managed within the project.

## Question 3

---

**Question Type:** MultipleChoice

---

Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

**Options:**

---

- A- Disaster Recovery Plan
- B- Contingency Plan
- C- Continuity Of Operations Plan
- D- Business Continuity Plan

**Answer:**

---

B

**Explanation:**

---

Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency

situation. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies

and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and 'triggers' for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.

Answer option A is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

Answer option C is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

Answer option D is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster

or extended disruption. The logistical plan is called a business continuity plan.

## Question 4

---

**Question Type:** MultipleChoice

---

Which of the following sites are similar to the hot site facilities, with the exception that they are completely dedicated, self-developed recovery facilities?

**Options:**

---

- A- Cold sites
- B- Orange sites
- C- Warm sites
- D- Duplicate processing facilities

**Answer:**

---

D

**Explanation:**

---

The duplicate processing facilities work in the same manner as the hot site facilities, with the exception that they are completely dedicated, self-developed recovery facilities. The duplicate facility holds same equipment, operating systems, and applications and might have regularly synchronized data. The examples of the duplicate processing facilities can be the large organizations that have multiple geographic locations.

Answer option A is incorrect. A cold site is a backup site in case disaster has taken place in a data center. This is the least expensive disaster recovery solution, usually having only a single room with no equipment. All equipment is brought to the site after the disaster. It



can be on site or off site.

Answer option C is incorrect. A warm site is, quite logically, a compromise between hot and cold sites. Warm sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. These sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

Answer option B is incorrect. This is not a valid recovery site.

## Question 5

---

**Question Type:** MultipleChoice

---

Which of the following divisions of the Trusted Computer System Evaluation Criteria (TCSEC) is based on the Mandatory Access Control (MAC) policy?

### Options:

---

A- Division A

B- Division D

**C-** Division B

**D-** Division C

**Answer:**

---

C

**Explanation:**

---

Division B of the Trusted Computer System Evaluation Criteria (TCSEC) is based on the Mandatory Access Control (MAC) policy. Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as 'secret', he cannot grant permission to other users to see this object unless they have the appropriate permission.

## Question 6

---

**Question Type:** MultipleChoice

---

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

### Options:

---

- A- Senior Management
- B- Business Unit Manager
- C- Information Security Steering Committee
- D- Chief Information Security Officer

### Answer:

---

A

### Explanation:

---

Senior management provides management, operational and technical controls to satisfy security requirements. The governance roles and responsibilities are mentioned below in the table.

## Question 7

---

**Question Type:** MultipleChoice

---

Which of the following measurements of an enterprise's security state is the process whereby an organization establishes the parameters within which programs, investments, and acquisitions reach the desired results?

**Options:**

---

- A- Information sharing
- B- Ethics
- C- Performance measurement
- D- Risk management

**Answer:**

---

C

**Explanation:**

---

Performance measurement is the process whereby an organization establishes the parameters within which programs, investments, and acquisitions reach the desired results. This process of measuring performance often requires the use of statistical evidence to determine progress toward specific defined organizational objectives. Fundamental purpose behind measures is to improve performance. This is conducted with the same rigor as for other enterprise business units, functions, and processes.

Answer option D is incorrect. Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the

realization of opportunities.

Answer option B is incorrect. Ethics are the rules of personal behavior.

Answer option A is incorrect. Information sharing includes ensuring that the right information is collected, retained, and communicated to the right parties at the right time.

## Question 8

---

**Question Type:** MultipleChoice

---

Which of the following liabilities is a third-party liability in which an individual may be responsible for an action by another party?

### Options:

---

- A- Relational liability
- B- Engaged liability
- C- Contributory liability
- D- Vicarious liability

**Answer:**

---

D

**Explanation:**

---

Vicarious liability is based on the doctrine of respondeat superior, where a superior is responsible for the actions of a subordinate.

Vicarious liability is a form of strict, secondary liability that arises under the common law doctrine of agency, respondeat superior, the responsibility of the superior for the acts of their subordinate, or, in a broader sense, the responsibility of any third party that had the 'right, ability or duty to control' the activities of a violator.

Answer option C is incorrect. Contributory liability or contributory infringement has been widely defined as a form of liability on the part of someone who is not directly infringing but nevertheless is making contributions to the infringing acts of others. Contributory liability is rooted

in the tort theory of enterprise liability. Contributory liability holds the third party liable for the primary act by virtue of the third party's relationship with the actual harm (either by enabling it or benefiting from it).

Answer options A and B are incorrect. These are not valid options.

**To Get Premium Files for ISSMP Visit**

<https://www.p2pexams.com/products/issmp>

**For More Free Questions Visit**

<https://www.p2pexams.com/isc2/pdf/issmp>

