Examcollection

http://www.ipass4sure.com/examcollection.htm

http://www.ipass4sure.com

CSSLP

ISC2

Certified Secure Software Lifecycle Professional

http://www.ipass4sure.com/exams.asp?examcode=CSSLP

The CSSLP practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The CSSLP Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently.
The CSSLP exam is very challenging, but with our CSSLP questions and answers practice exam, you can feel confident in obtaining your success on the CSSLP exam on your FIRST TRY!

ISC2 CSSLP Exam Features

- Detailed questions and answers for CSSLP exam
- Try a demo before buying any ISC2 exam
- CSSLP questions and answers, updated regularly
- Verified CSSLP answers by Experts and bear almost 100% accuracy
- CSSLP tested and verified before publishing
- CSSLP examcollection vce questions with exhibits
- CSSLP same questions as real exam with multiple choice options

Acquiring ISC2 certifications are becoming a huge task in the field of I.T. More over these exams like CSSLP exam are now continuously updating and accepting this challenge is itself a task. This CSSLP test is an important part of ISC2 certifications. We have the resources to prepare you for this. The CSSLP exam is essential and core part of ISC2 certifications and once you clear the exam you will be able to solve the real life problems yourself.Want to take advantage of the Real CSSLP Test and save time and money while developing your skills to pass your ISC2 CSSLP Exam? Let us help you climb that ladder of success and pass your CSSLP now!

DEMO EXAM

For Full Version visit

http://www.ipass4sure.com/allexams.asp

QUESTION: 1
You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

A. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
B. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.
C. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
D. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.

Answer: B

Explanation:
Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process.
Answer option A is incorrect. This is actually the definition of qualitative risk analysis.
Answer option D is incorrect. While somewhat true, this statement does not completely define the quantitative risk analysis process.
Answer option C is incorrect. This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.

QUESTION: 2
Fill in the blank with the appropriate security mechanism._____ is a computer hardware mechanism or programming language construct which handles the occurrence of exceptional events.

Answer:
Exception handling

Explanation:
Exception handling is a computer hardware mechanism or programming language construct that handles the occurrence of events. These events occur during the software execution process and interrupt the instruction flow. Exception handling performs the specific activities for managing the exceptional events.

QUESTION: 3
In which type of access control do user ID and password system come under?

A. Physical
B. Administrative
C. Technical
D. Power

Answer: C

Explanation:
Technical access controls include IDS systems, encryption, network segmentation, and antivirus controls.
Answer option B is incorrect. The policies and procedures implemented by an organization come under administrative access controls.
Answer option A is incorrect. Security guards, locks on the gates, and alarms come under physical access controls.
Answer option D is incorrect. There is no such type of access control as power control.

QUESTION: 4
You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

A. Three
B. Four
C. Seven
D. One

Answer: B

Explanation:
There are four risk responses available for a negative risk event. The risk response strategies for negative risks are:
Avoid: It involves altering the project management plan to remove the threats completely. Transfer: It requires shifting some or all of the negative effects of a threat including the ownership of response, to a third party.
Mitigate: It implies a drop in the probability and impact of an unfavorable risk event to be within suitable threshold limits.
Accept: It delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk occurs. It is used for both negative and positive risks.
Answer option D is incorrect. There are four responses for negative risk events.
Answer option A is incorrect. There are four, not three, responses for negative risk events. Do not forget that acceptance can be used for negative risk events.

Answer option C is incorrect. There are seven total risk responses, four of which can be used for negative risk events.

QUESTION: 5
What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

A. Conduct activities related to the disposition of the system data and objects.
B. Conduct validation activities.
C. Execute and update IA implementation plan.
D. Combine validation results in DIACAP scorecard.

Answer: B,C,D

Explanation:
The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk.The subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process are as follows:
Execute and update IA implementation plan. Conduct validation activities.
Combine validation results in the DIACAP scorecard.
Answer option A is incorrect. The activities related to the disposition of the system data and objects are conducted in the fifth phase of the DIACAP process. The fifth phase of the DIACAP process is known as Decommission System.

QUESTION: 6
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

A. Confidentiality
B. Availability
C. Integrity
D. Encryption

Answer: A

Explanation:

The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security. Confidentiality is the concern that data be secure from unauthorized access.
Answer options B and C are incorrect. The CIA (Confidentiality, Integrity, and Availability) triangle is concerned with three facets of security.
Integrity is the concern that data not be altered without it being traceable. Availability is the concern that the data, while being secured, is readily accessible.
Answer option D is incorrect. Confidentiality may be implemented with encryption but encryption is just a technique to obtain confidentiality.

QUESTION: 7
Which of the following scanning techniques helps to ensure that the standard software configuration is currently with the latest security patches and software, and helps to locate uncontrolled or unauthorized software?

A. Workstation Scanning
B. Server Scanning
C. Port Scanning
D. Discovery Scanning

Answer: A

Explanation:
Workstation scanning provides help to ensure that the standard software configuration exists with the most recent security patches and software. It helps to locate uncontrolled or unauthorized software.A full workstation vulnerability scan of the standard corporate desktop configuration must be implemented on a regularly basis.
Answer option D is incorrect. The discovery scanning technique is used to gather adequate information regarding each network device to identify what type of device it is, its operating system, and if it is running any externally vulnerable services, like Web services, FTP, or email.
Answer option B is incorrect. A full server vulnerability scan helps to determine if the server OS has been configured to the corporate standards and identify if applications have been updated with the latest security patches and software versions.
Answer option C is incorrect. Port scanning technique describes the process of sending a data packet to a port to gather information about the state of the port.

QUESTION: 8
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

A. Transference
B. Avoidance
C. Mitigation
D. Exploit

Answer: A

Explanation:
When you are hiring a third party to own risk, it is known as transference risk response. Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference.
Answer option C is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation.
Answer option D is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized.
Answer option B is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

QUESTION: 9
The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented?Each correct answer represents a complete solution. Choose all that apply.

A. Configuration change control
B. Configuration implementation
C. Configuration deployment
D. Configuration status accounting
E. Configuration audits
F. Configuration identification

Answer: A,D,E,F

Explanation:
The SCM process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are as follows:

1. Configuration identification: Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined.
2. Configuration change control: Configuration change control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them.
3. Configuration status accounting: Configuration status accounting is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.
4. Configuration audits: Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

QUESTION: 10
Which of the following plans is designed to protect critical business processes from natural or man- made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

A. Crisis communication plan
B. Business continuity plan
C. Contingency plan
D. Disaster recovery plan

Answer: B

Explanation:
The business continuity plan is designed to protect critical business processes from natural or man- made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes. 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.
Answer option A is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation.The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or

event driven circumstances. Answer option C is incorrect. 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 D 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.

QUESTION: 11
You work as a security engineer for BlueWell Inc. According to you, which of the following DITSCAP/NIACAP model phases occurs at the initiation of the project, or at the initial C&A effort of a legacy system?

A. Definition
B. Post Accreditation
C. Verification
D. Validation

Answer: A

Explanation:
The definition phase of the DITSCAP/NIACAP model takes place at the beginning of the project, or at the initial C&A effort of a legacy system.C&A consists of four phases in a DITSCAP assessment. These phases are the same as NIACAP phases. The order of these phases is as follows:
1. Definition: The definition phase is focused on understanding the IS business case, the mission, environment, and architecture. This phase determines the security requirements and level of effort necessary to achieve Certification & Accreditation (C&A).
2. Verification: The second phase confirms the evolving or modified system's compliance with the information. The verification phase ensures that the fully integrated system will be ready for certification testing.
3. Validation: The third phase confirms abidance of the fully integrated system with the security policy. This phase follows t requirements slated in the SSAA. The objective of the validation phase is to show the required evidence to support the DAA in accreditation process.
4. Post Accreditation: The Post Accreditation is the final phase of DITSCAP assessment and it starts after the system has been certified and accredited for operations. This phase

ensures secure system management, operation, and maintenance to save an acceptable level of residual risk.

QUESTION: 12
Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing? Each correct answer represents a complete solution. Choose all that apply.

A. Zero-knowledge test
B. Open-box
C. Full-knowledge test
D. Full-box
E. Closed-box
F. Partial-knowledge test

Answer: A,B,C,E,F

Explanation:
The different categories of penetration testing are as follows:
Open-box: In this category of penetration testing, testers have access to internal system code. This mode is basically suited for Unix or Linux.
Closed-box: In this category of penetration testing, testers do not have access to closed systems. This method is good for closed systems.
Zero-knowledge test: In this category of penetration testing, testers have to acquire information from scratch and they are not supplied with information concerning the IT system.
Partial-knowledge test: In this category of penetration testing, testers have knowledge that may be applicable to a specific type of attack and associated vulnerabilities.
Full-knowledge test: In this category of penetration testing, testers have massive knowledge concerning the information system to be evaluated.
Answer option D is incorrect. There is no such category of penetration testing.

QUESTION: 13
Which of the following refers to a process that is used for implementing information security?

A. Information Assurance (IA)
B. Certification and Accreditation (C&A)
C. Five Pillars model
D. Classic information security model

Answer: B

Explanation:
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3.Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.Answer option A is incorrect. Information Assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computer security.
Answer option D is incorrect. The classic information security model is used in the practice of Information Assurance (IA) to define assurance requirements. The classic information security model, also called the CIA Triad, addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance.
Answer option C is incorrect. The Five Pillars model is used in the practice of Information Assurance
(IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

QUESTION: 14

Pass4sure Certification Exam Features;

- Pass4sure offers over **2500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **120** Global Certification Vendors Covered.
- Services of Professional & Certified Experts available via support.
- Free 90 days updates to match real exam scenarios.
- Instant Download Access! No Setup required.
- Price as low as $19, which is 80% more cost effective than others.
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (Android, iPhone, iPod, iPad)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- ***Guaranteed Success***.
- **Fast**, helpful support 24x7.

View list of All certification exams offered;
http://www.ipass4sure.com/allexams.asp

View list of All Study Guides (SG);
http://www.ipass4sure.com/study-guides.asp

View list of All Audio Exams (AE);
http://www.ipass4sure.com/audio-exams.asp

Download Any Certication Exam DEMO.
http://www.ipass4sure.com/samples.asp

To purchase Full version of exam click below;
http://www.ipass4sure.com/allexams.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

and many others.. See complete list Here