CISSP

ISC2

Certified Information Systems Security Professional

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=CISSP

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your CISSP exam in first attempt, but also you can get a high score to acquire ISC2 certification.

If you use pass4sureofficial CISSP Certification questions and answers, you will experience actual CISSP exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our ISC2 exam prep covers over 95% of the questions and answers that may be appeared in your CISSP exam. Every point from pass4sure CISSP PDF, CISSP review will help you take ISC2 CISSP exam much easier and become ISC2 certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial ISC2 CISSP course:

** Up-to-Date ISC2 CISSP questions taken from the real exam.*
** 100% correct ISC2 CISSP answers you simply can't find in other CISSP courses.*
** All of our tests are easy to download. Your file will be saved as a CISSP PDF.*
** ISC2 CISSP brain dump free content featuring the real CISSP test questions.*

ISC2 CISSP certification exam is of core importance both in your Professional life and ISC2 certification path. With ISC2 certification you can get a good job easily in the market and get on your path for success. Professionals who passed ISC2 CISSP exam training are an absolute favorite in the industry. You will pass ISC2 CISSP certification test and career opportunities will be open for you.

QUESTION: 1
Which statement below is accurate about the difference between issuespecific and system-specific policies?

A. Issue-specific policy is much more technically focused.
B. System-specific policy is much more technically focused.
C. System-specific policy is similar to program policy.
D. Issue-specific policy commonly addresses only one system.

Answer: B

Explanation:
Often, managerial computer system security policies are categorized into three basic types:
Program policyÑused to create an organizationês computer security program
Issue-specific policiesÑused to address specific issues of concern to the organization
System-specific policiesÑtechnical directives taken by management to protect a particular system
Program policy and issue-specific policy both address policy from
a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. System-specific policy fills this need. System-specific policy is much more focused, since it addresses only one system.Table A.1 helps illustrate the difference between these three types of policies.

Reference:
National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook Special Publica- tion 800-12.

Security Policy Types

POLICY TYPE	DESCRIPTION	EXAMPLE
Program policy	High-level program policy	Senior-level Management Statement
Issue-specific policy	Addresses single issue	Email privacy policy
System-specific policy	Single-system directives	Router Access Control Lists

QUESTION: 2

Which statement below most accurately describes the difference between security awareness, security training, and security education?

A. Security training teaches the skills that will help employees to perform their jobs more securely.
B. Security education is required for all system operators.
C. Security awareness is not necessary for high-level senior executives.
D. Security training is more in depth than security education.

Answer: A

Explanation:
Awareness is used to reinforce the fact that security supports the mission of the organization by protecting valuable resources. The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. Security education is more in depth than security training and is targeted for security professionals and those whose jobs require expertise in security. Management commitment is necessary because of the resources used in developing and implementing the program and also because the program affects their stafF.

Reference:
National Institute of Standards and Technology, An Introduction to Computer Security: The NIST Handbook Special Publica- tion 800-12.

QUESTION: 3
Which choice below BEST describes the difference between the System Owner and the Information Owner?

A. There is a one-to-one relationship between system owners and information owners.
B. One system could have multiple information owners.
C. The Information Owner is responsible for defining the systemês operating parameters.
D. The System Owner is responsible for establishing the rules for appropriate use of the information.

Answer: B

Explanation:
The System Owner is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. The System Owner is responsible for defining the systemês operating parameters, authorized functions, and

security requirements. The information owner for information stored within, processed by, or transmitted by a system may or may not be the same as the System Owner. Also, a single system may utilize information from multiple Information Owners.The Information Owner is responsible for establishing the rules for appropriate use and protection of the subject data/information (rules of behavior). The Information Owner retains that responsibility even when the data/information are shared with other organizations.

Reference:
NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.

QUESTION: 4
Which choice below is NOT an accurate statement about an organizationês incident-handling capability?

A. The organizationês incident-handling capability should be used to detect and punish senior-level executive wrong-doing.
B. It should be used to prevent future damage from incidents.
C. It should be used to provide the ability to respond quickly and effectively to an incident.
D. The organizationês incident-handling capability should be used to contain and repair damage done from incidents.

Answer: A

Explanation:
An organization should address computer security incidents by developing an incident-handling capability. The incident-handling capability should be used to:Provide the ability to respond quickly and effectively. Contain and repair the damage from incidents. When left unchecked, malicious software can significantly harm an organizationês computing, depending on the technology and its connectivity. Containing the incident should include an assessment of whether the incident is part of a targeted attack on the organization or an isolated incident.Prevent future damagE. An incident-handling capability should assist an organization in preventing (or at least minimizing) damage from future incidents. Incidents can be studied internally togain a better understanding of the organizationês threats and vulnerabilities.

Reference:

NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.

QUESTION: 5
Place the data classification scheme in order, from the least secure to the most:

A. Sensitive
B. Public
C. Private
D. Confidential

Answer: A,B,C,D

Explanation:
Various formats for categorizing the sensitivity of data exist. Although originally implemented in government systems, data classification is

A Sample H/M/L Data Classification

CATEGORY	DESCRIPTION
High	Could cause loss of life, imprisonment, major financial loss, or require legal action for correction if the information is compromised.
Medium	Could cause significant financial loss or require legal action for correction if the information is compromised.
Low	Would cause only minor financial loss or require only administrative action for correction if the information is compromised.

very useful in determining the sensitivity of business information to threats to confidentiality, integrity, or availability. Often an organization would use the high, medium, or low categories. This simple classification scheme rates each system by its need for protection based upon its C.I.A. needs, and whether it requires high, medium, or low protective controls. For example, a system and its information may require a high degree of integrity and availability, yet have no need for confidentiality.Or organizations may categorize data into four sensitivity classifications with separate handling requirements, such as Sensitive, Confidential, Private, and Public.This system would define the categories as follows:
Sensitive. This classification applies to information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher-than-normal assurance of accuracy and completeness.
Confidential. This classification applies to the most sensitive business information that is intended strictly for use within the organization.

Its unauthorized disclosure could seriously and adversely impact the organization, its stockholders, its business partners,
and/or its customers. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations.
PrivatE. This classification applies to personal information that is intended for use within the organization. Its unauthorized disclosure could seriously and adversely impact the organization and/or its employees.
Public. This classification applies to all other information that does not clearly fit into any of the preceding three classifications.
While its unauthorized disclosure is against policy, it is not expected to impact seriously or adversely the organization, its employees, and/or its customers.
The designated owners of information are responsible for determining data classification levels, subject to executive
management review. Table shows a sample H/M/L data classification for sensitive information.

Reference:
NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

A Sample H/M/L Data Classification

CATEGORY	DESCRIPTION
High	Could cause loss of life, imprisonment, major financial loss, or require legal action for correction if the information is compromised.
Medium	Could cause significant financial loss or require legal action for correction if the information is compromised.
Low	Would cause only minor financial loss or require only administrative action for correction if the information is compromised.

QUESTION: 6
CORRECT TEXT
Place the five system security life-cycle phases in order:

A. Implementation phase
B. Development/acquisition phase
C. Disposal phase
D. Operation/maintenance phase
E. Initiation phase

Answer: E, B, A, D, C

QUESTION: 7
How often should an independent review of the security controls be performed, according to OMB Circular A-130?

A. Every year
B. Every three years
C. Every five years
D. Never

Answer: B

Explanation:
The correct answer is B. OMB Circular A-130 requires that a review of the security controls for each major government application be performed at least every three years. For general support systems, OMB Circular A-130 requires that the security controls be reviewed either by an independent audit or self review. Audits can be selfadministered or independent (either internal or external). The essential difference between a self-audit and an independent audit is objectivity; however, some systems may require a fully independent review.

Reference:
Office of Management and Budget Circular A-130, revised November 30, 2000 .

QUESTION: 08
Which choice below is NOT one of NISTês 33 IT security principles?

A. Implement least privilege.
B. Assume that external systems are insecure.
C. Totally eliminate any level of risk.
D. Minimize the system elements to be trusted.

Answer: C

Explanation:
Risk can never be totally eliminateD. NIST IT security principle #4 states: çReduce risk to an acceptable level.é The National Institute of Standards and Technologyês (NIST) Information Technology Laboratory (ITL) released NIST Special Publication

(SP) 800-27, çEngineering Principles for Information Technology Security (EP-ITS)é in June 2001 to assist in the secure design, development, deployment, and life-cycle of information systems. It presents 33 security principles which start at the design phase of the information system or application and continue until the systemês retirement and secure disposal.Some of the other 33 principles are:
Principle 1. Establish a sound security policy as the çfoundationé for design.
Principle 2. Treat security as an integral part of the overall system design.
Principle 5. Assume that external systems are insecure.
Principle 6. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
Principle 7. Implement layered security (ensure no single point of vulnerability).
Principle 11. Minimize the system elements to be trusted.
Principle 16. Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
Principle 17. Use boundary mechanisms to separate computing systems and network infrastructures.
Principle 22. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
Principle 23. Use unique identities to ensure accountability. Principle 24. Implement least privilege.

Reference:
NIST Special Publication 800-27, Engineering Principles for Infor- mation Technology Security (A Baseline for Achieving Security), and çFederal Systems Level Guidance for Securing Information Systems,é James Corrie, August 16, 2001 .

QUESTION: 9
Which choice below would NOT be considered an element of proper user account management?

A. Users should never be rotated out of their current duties.
B. The usersê accounts should be reviewed periodically.
C. A process for tracking access authorizations should be implemented.
D. Periodically re-screen personnel in sensitive positions.

Answer: A

Explanation:
Organizations should ensure effective administration of usersê computer access to maintain system security, including user account management, auditing, and the timely modification or removal of access. This includes:

User Account Management. Organizations should have a process for requesting, establishing, issuing, and closing user accounts, tracking users and their respective access authorizations, and managing these functions.
Management Reviews. It is necessary to periodically review user accounts. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, and whether required training has been completed.
Detecting Unauthorized/Illegal Activities. Mechanisms besides auditing and analysis of audit trails should be used to detect unauthorized and illegal acts, such as rotating employees in sensitive positions, which could expose a scam that required an employeeês presence, or periodic re-screening of personnel.

Reference:
NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.

QUESTION: 10
Which question below is NOT accurate regarding the process of risk assessment?

A. The likelihood of a threat must be determined as an element of the risk assessment.
B. The level of impact of a threat must be determined as an element of the risk assessment.
C. Risk assessment is the first process in the risk management methodology
D. Risk assessment is the final result of the risk management methodology.

Answer: D

Explanation:
Risk is a function of the likelihood of a given threat-sourceês exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. Risk assessment is the first process in the risk management methodology. The risk assessment process helps organizations identify appropriate controls for reducing or eliminating risk during the risk mitigation process.To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. The likelihood that a potential vulnerability could be exercised by a given threat source can be described as high, medium, or low. Impact refers to the magnitude of harm that could be caused by a threatês exploitation of a vulnerability. The determination of the level of impact produces a relative value for the IT assets and resources affected.

Reference:
NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.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	SNIA