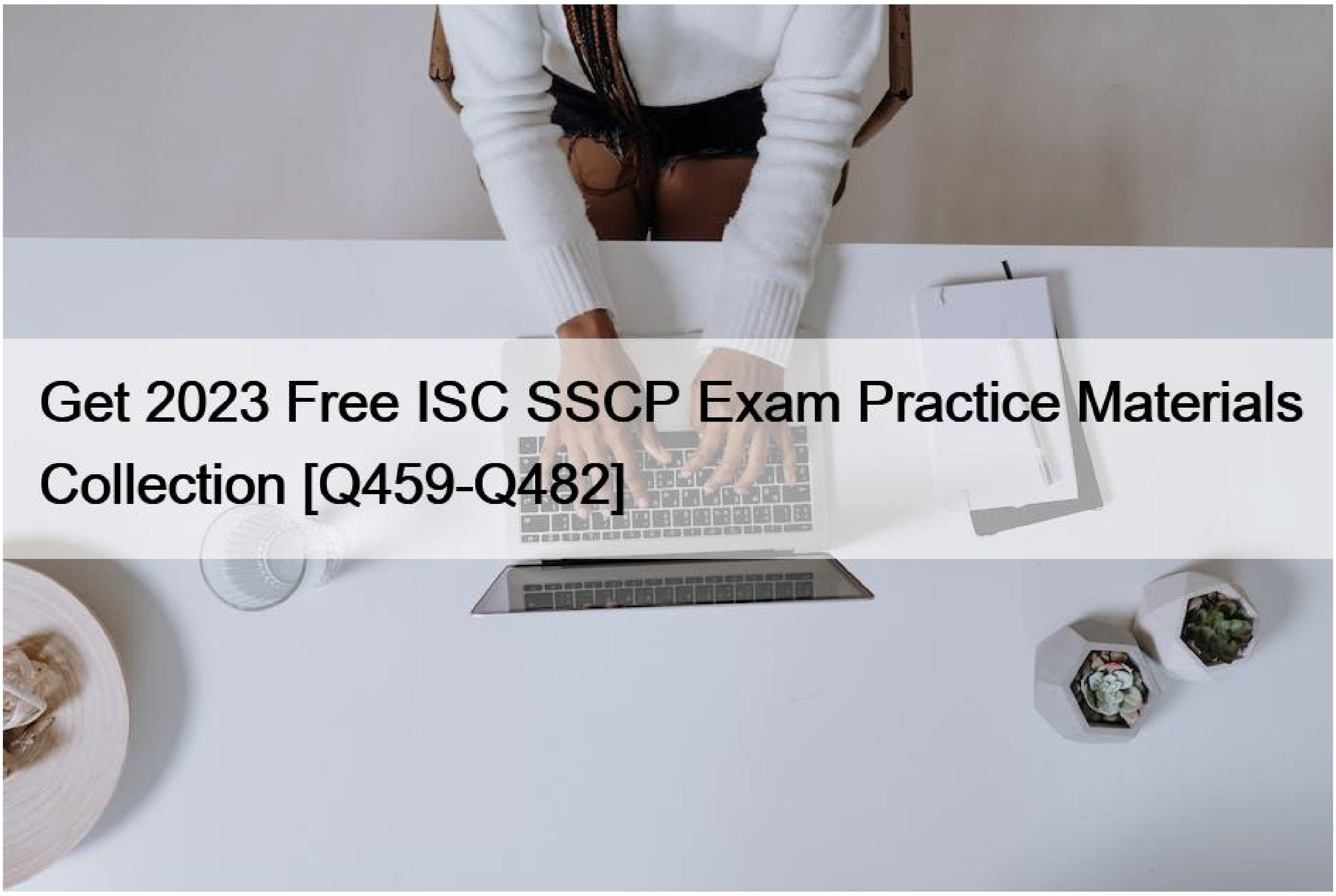
Get 2023 Free ISC SSCP Exam Practice Materials Collection [Q459-Q482



Get 2023 Free ISC SSCP Exam Practice Materials Collection Get Latest and 100% Accurate SSCP Exam Questions NO.459
Which of the following control pairings include: organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?
* Preventive/Administrative Pairing
* Preventive/Technical Pairing
* Preventive/Physical Pairing
* Detective/Administrative Pairing
Section: Access Control

Explanation/Reference:

The Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NO.460 Which of the following is the core of fiber optic cables made of?

* PVC
* Glass fibers
* Kevlar
* Teflon

Fiber optic cables have an outer insulating jacket made of Teflon or PVC, Kevlar fiber, which helps to strengthen the cable and prevent breakage, plastic coatings, used to cushion the fiber center. The center (core) of the cable is made of glass or plastic fibers.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 3: Telecommunications and Network Security (page 31).

NO.461 Which of the following is the core of fiber optic cables made of?

* PVC
* Glass fibers
* Kevlar
* Teflon

Explanation/Reference:

Fiber optic cables have an outer insulating jacket made of Teflon or PVC, Kevlar fiber, which helps to strengthen the cable and prevent breakage, plastic coatings, used to cushion the fiber center. The center (core) of the cable is made of glass or plastic fibers.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 3: Telecommunications and Network Security (page 31).

NO.462 Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?

* Internet Security Association and Key Management Protocol (ISAKMP)
* Simple Key-management for Internet Protocols (SKIP)
* Diffie-Hellman Key Distribution Protocol
* IPsec Key exchange (IKE)

RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as:

A key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated. SKIP uses the knowledge of its own secret key or private component and the destination&#8217;s public component to calculate a unique key that can only be used between them.

IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally. Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a Diffie-Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

The following are incorrect answers:

ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

IKE is an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

IPsec Key exchange (IKE) is only a detracto.

Reference(s) used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000. and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

NO.463 What does &#8220;residual risk&#8221; mean?
* The security risk that remains after controls have been implemented
* Weakness of an assets which can be exploited by a threat
* Risk that remains after risk assessment has has been performed
* A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Residual risk is &#8220;The security risk that remains after controls have been implemented&#8221; ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and Models for IT Security, 1996. &#8220;Weakness of an assets which can be exploited by a threat&#8221; is vulnerability. &#8220;The result of unwanted incident&#8221; is impact. Risk that remains after risk analysis has been performed is a distracter.

Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.

NO.464 The IDEA algorithm (used in PGP) is _______ bits long.
* 56
* 158
* 128
* 168

NO.465 This type of backup management provides a continuous on-line backup by using optical or tape &#8220;jukeboxes,&#8221; similar to WORMs (Write Once, Read Many):
* Hierarchical Storage Management (HSM).
* Hierarchical Resource Management (HRM).
* Hierarchical Access Management (HAM).
* Hierarchical Instance Management (HIM).

Hierarchical Storage Management (HSM) provides a continuous on-line

backup by using optical or tape &#8220;jukeboxes,&#8221; similar to WORMs.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the

Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 71.

NO.466 Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:
* neither physical attacks nor attacks from malicious code.
* physical attacks only

* both physical attacks and attacks from malicious code.
* physical attacks but not attacks from malicious code.
Section: Access Control

Explanation/Reference:

Since all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to both physical attacks and attacks from malicious code.

Because a client&#8217;s password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42.

NO.467 Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?
* Authentication
* Administration
* Accounting
* Authorization
Section: Access Control

Explanation/Reference:

Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.

Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

also see:

The term &#8220;AAA&#8221; is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three &#8220;A&#8217;s&#8221; can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions.

Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

NO.468 Which security model is based on the military classification of data and people with clearances?
* Brewer-Nash model
* Clark-Wilson model
* Bell-LaPadula model
* Biba model
Section: Access Control

Explanation/Reference:

The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity.

Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

NO.469 The end result of implementing the principle of least privilege means which of the following?
* Users would get access to only the info for which they have a need to know
* Users can access all systems.
* Users get new privileges added when they change positions.
* Authorization creep.
Explanation/Reference:

The principle of least privilege refers to allowing users to have only the access they need and not anything more. Thus, certain users may have no need to access any of the files on specific systems.

The following answers are incorrect:

Users can access all systems. Although the principle of least privilege limits what access and systems users have authorization to, not all users would have a need to know to access all of the systems. The best answer is still Users would get access to only the info for which they have a need to know as some of the users may not have a need to access a system.

Users get new privileges when they change positions. Although true that a user may indeed require new privileges, this is not a given fact and in actuality a user may require less privileges for a new position. The principle of least privilege would require that the rights required for the position be closely evaluated and where possible rights revoked.

Authorization creep. Authorization creep occurs when users are given additional rights with new positions and responsibilities. The principle of least privilege should actually prevent authorization creep.

The following reference(s) were/was used to create this question:

ISC2 OIG 2007 p.101,123

Shon Harris AIO v3 p148, 902-903

NO.470 What size is an MD5 message digest (hash)?
* 128 bits
* 160 bits
* 256 bits
* 128 bytes
Explanation/Reference:

MD5 is a one-way hash function producing a 128-bit message digest from the input message, through 4 rounds of transformation. MD5 is specified as an Internet Standard (RFC1312).

Reference(s) used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NO.471 There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?
* public keys
* private keys

* public-key certificates
* private-key certificates
Section: Access Control

Explanation/Reference:

A Kerberos ticket is issued by a trusted third party. It is an encrypted data structure that includes the service encryption key. In that sense it is similar to a public-key certificate. However, the ticket is not the key.

The following answers are incorrect:

public keys. Kerberos tickets are not shared out publicly, so they are not like a PKI public key.

private keys. Although a Kerberos ticket is not shared publicly, it is not a private key. Private keys are associated with Asymmetric crypto system which is not used by Kerberos. Kerberos uses only the Symmetric crypto system.

private key certificates. This is a detractor. There is no such thing as a private key certificate.

NO.472 Which of the following statements pertaining to link encryption is false?
* It encrypts all the data along a specific communication path.
* It provides protection against packet sniffers and eavesdroppers.
* Information stays encrypted from one end of its journey to the other.
* User information, header, trailers, addresses and routing data that are part of the packets are encrypted.
Section: Network and Telecommunications

Explanation/Reference:

When using link encryption, packets have to be decrypted at each hop and encrypted again.

Information staying encrypted from one end of its journey to the other is a characteristic of end-to-end encryption, not link encryption.

Link Encryption vs. End-to-End Encryption

Link encryption encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.

End-to-end encryption does not encrypt the IP Protocol headers, and therefore does not need to be decrypted at each hop.

Reference: All in one, Page 735 & Glossary

and

Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

NO.473 How are memory cards and smart cards different?
* Memory cards normally hold more memory than smart cards
* Smart cards provide a two-factor authentication whereas memory cards don&#8217;t
* Memory cards have no processing power
* Only smart cards can be used for ATM cards
Explanation/Reference:

The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process that information.

A memory card holds a user&#8217;s authentication information, so that this user needs only type in a user ID or PIN and presents the memory card to the system. If the entered information and the stored information match and are approved by an authentication service, the user is successfully authenticated.

A common example of a memory card is a swipe card used to provide entry to a building. The user enters a PIN and swipes the memory card through a card reader. If this is the correct combination, the reader flashes green and the individual can open the door and enter the building.

Memory cards can also be used with computers, but they require a reader to process the information. The reader adds cost to the process, especially when one is needed for every computer. Additionally, the overhead of PIN and card generation adds additional overhead and complexity to the whole authentication process. However, a memory card provides a more secure authentication method than using only a password because the attacker would need to obtain the card and know the correct PIN.

Administrators and management need to weigh the costs and benefits of a memory card implementation as well as the security needs of the organization to determine if it is the right authentication mechanism for their environment.

One of the most prevalent weaknesses of memory cards is that data stored on the card are not protected.

Unencrypted data on the card (or stored on the magnetic strip) can be extracted or copied. Unlike a smart card, where security controls and logic are embedded in the integrated circuit, memory cards do not employ an inherent mechanism to protect the data from exposure.

Very little trust can be associated with confidentiality and integrity of information on the memory cards.

The following answers are incorrect:

&#8220;Smart cards provide two-factor authentication whereas memory cards don&#8217;t&#8221; is incorrect. This is not necessarily true. A memory card can be combined with a pin or password to offer two factors authentication where something you have and something you know are used for factors.

&#8220;Memory cards normally hold more memory than smart cards&#8221; is incorrect. While a memory card may or may not have more memory than a smart card, this is certainly not the best answer to the question.

&#8220;Only smart cards can be used for ATM cards&#8221; is incorrect. This depends on the decisions made by the particular institution and is not the best answer to the question.

Reference(s) used for this question:

Shon Harris, CISSP All In One, 6th edition , Access Control, Page 199 and also for people using the Kindle edition of the book you can look at Locations 4647-4650.

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 2124-2139). Auerbach Publications. Kindle Edition.

NO.474 An intrusion detection system is an example of what type of countermeasure?

* Preventative
* Corrective
* Subjective
* Detective
* Postulative

NO.475 There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?

* public keys
* private keys
* public-key certificates
* private-key certificates

A Kerberos ticket is issued by a trusted third party. It is an encrypted data

structure that includes the service encryption key. In that sense it is similar to a public-key

certificate. However, the ticket is not the key.

The following answers are incorrect:

public keys. Kerberos tickets are not shared out publicly, so they are not like a PKI public

key.

private keys. Although a Kerberos ticket is not shared publicly, it is not a private key.

Private keys are associated with Asymmetric crypto system which is not used by Kerberos.

Kerberos uses only the Symmetric crypto system.

private key certificates. This is a detractor. There is no such thing as a private key

certificate.

NO.476 Which of the following is a tool often used to reduce the risk to a local area network (LAN) that has external connections by filtering Ingress and Egress traffic?

* a firewall.
* dial-up.
* passwords.
* fiber optics.

Section: Network and Telecommunications

Explanation/Reference:

The use of a firewall is a requirement to protect a local area network (LAN) that has external connections without that you have no real protection from fraudsters.

The following answers are incorrect:

dial-up. This is incorrect because this offers little protection once the connection has been established.

passwords. This is incorrect because there are tools to crack passwords and once a user has been authenticated and connects to the external connections, passwords do not offer protection against incoming TCP packets.

fiber optics. This is incorrect because this offers no protection from the external connection.

NO.477 Which of the following is NOT an example of an operational control?
* backup and recovery
* Auditing
* contingency planning
* operations procedures

Explanation/Reference:

Operational controls are controls over the hardware, the media used and the operators using these resources.

Operational controls are controls that are implemented and executed by people, they are most often procedures.

Backup and recovery, contingency planning and operations procedures are operational controls.

Auditing is considered an Administrative / detective control. However the actual auditing mechanisms in place on the systems would be consider operational controls.

NO.478 Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?
* 10.0.42.5
* 11.0.42.5
* 12.0.42.5
* 13.0.42.5

This is a valid Class A reserved address. For Class A, the reserved addresses are 10.0.0.0 &#8211; 10.255.255.255.

The following answers are incorrect:

11.0.42.5

Is incorrect because it is not a Class A reserved address.

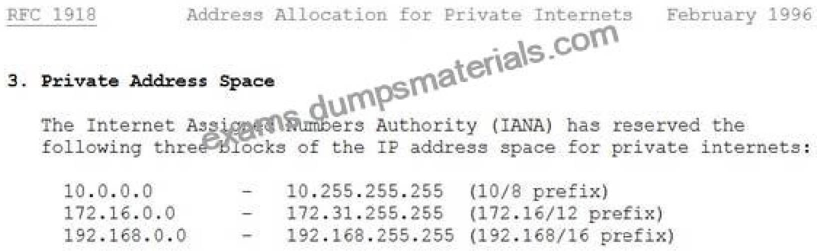
12.0.42.5

Is incorrect because it is not a Class A reserved address.

13.0.42.5

Is incorrect because it is not a Class A reserved address.

The private IP address ranges are defined within RFC 1918: RFC 1918 private ip address range



```
RFC 1918       Address Allocation for Private Internets   February 1996

3. Private Address Space

   The Internet Assigned Numbers Authority (IANA) has reserved the
   following three blocks of the IP address space for private internets:

     10.0.0.0        -   10.255.255.255  (10/8 prefix)
     172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
     192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

References: 3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf

AIOv3 Telecommunications and Networking Security (page 438)

NO.479 Which of the following statements pertaining to VPN protocol standards is false?
* L2TP is a combination of PPTP and L2F.
* L2TP and PPTP were designed for single point-to-point client to server communication.
* L2TP operates at the network layer.
* PPTP uses native PPP authentication and encryption services.

L2TP and PPTP were both designed for individual client to server connections; they enable only a single point-to-point connection per session. Dial-up VPNs use L2TP often. Both L2TP and PPTP operate at the data link layer (layer 2) of the OSI model. PPTP uses native PPP authentication and encryption services and L2TP is a combination of PPTP and Layer 2 Forwarding protocol (L2F).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 95).

NO.480 Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:
* through access control mechanisms that require identification and authentication and through the audit function.
* through logical or technical controls involving the restriction of access to systems and the protection of information.
* through logical or technical controls but not involving the restriction of access to systems and the protection of information.
* through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Section: Access Control

Explanation/Reference:

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization&#8217;s security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NO.481 In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?
* Using a write blocker
* Made a full-disk image
* Created a message digest for log files

- Displayed the contents of a folder

Displaying the directory contents of a folder can alter the last access time on each listed file.

Using a write blocker is wrong because using a write blocker ensure that you cannot modify the data on the host and it prevent the host from writing to its hard drives.

Made a full-disk image is wrong because making a full-disk image can preserve all data on a hard disk, including deleted files and file fragments.

Created a message digest for log files is wrong because creating a message digest for log files. A message digest is a cryptographic checksum that can demonstrate that the integrity of a file has not been compromised (e.g. changes to the content of a log file)

Domain: LEGAL, REGULATIONS, COMPLIANCE AND INVESTIGATIONS

References: AIO 3rd Edition, page 783-784 NIST 800-61 Computer Security Incident Handling guide page 3-18 to 3-20

NO.482 Which of the following is the BEST way to detect software license violations?

- Implementing a corporate policy on copyright infringements and software use.
- Requiring that all PCs be diskless workstations.
- Installing metering software on the LAN so applications can be accessed through the metered software.
- Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.

The best way to prevent and detect software license violations is to regularly scan used PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.

Other options are not detective.

A corporate policy is not necessarily enforced and followed by all employees.

Software can be installed from other means than floppies or CD-ROMs (from a LAN or even downloaded from the Internet) and software metering only concerns applications that are registered. Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).