The following answers are incorrect:

The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

References:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Online_transaction_processing and
http://databases.about.com/od/administration/g/concurrency.htm

QUESTION 459
What is the essential difference between a self-audit and an independent audit?

A. Tools used
B. Results
C. Objectivity
D. Competence

Correct Answer: C
Explanation:
To maintain operational assurance, organizations use two basic methods:
system audits and monitoring. Monitoring refers to an ongoing activity whereas audits are one-time or periodic events and can be either internal or external. The essential difference between a self-audit and an independent audit is objectivity, thus indirectly affecting the results of the audit. Internal and external auditors should have the same level of competence and can use the same tools.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 25).

QUESTION 460
Which of the following Intrusion Detection Systems (IDS) uses a database of attacks, known system vulnerabilities, monitoring current attempts to exploit those vulnerabilities, and then triggers an alarm if an attempt is found?

A. Knowledge-Based ID System
B. Application-Based ID System
C. Host-Based ID System
D. Network-Based ID System

Correct Answer: A
Explanation:

Knowledge-based Intrusion Detection Systems use a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities, and trigger an alarm if an attempt is found.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

Application-Based ID System - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87

Host-Based ID System - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host."

Source: Official ISC2 Guide to the CISSP CBK - p. Network-Based ID System - "a network device, or dedicated system attached to teh network, that monitors traffic traversing teh network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196

QUESTION 461
The session layer provides a logical persistent connection between peer hosts. Which of the following is one of the modes used in the session layer to establish this connection?

A. Full duplex
B. Synchronous
C. Asynchronous
D. Half simplex

Correct Answer: A
Explanation:
Layer 5 of the OSI model is the Session Layer. This layer provides a logical persistent connection between peer hosts. A session is analogous to a conversation that is necessary for applications to exchange information.

The session layer is responsible for establishing, managing, and closing end-to-end connections, called sessions, between applications located at different network endpoints. Dialogue control management provided by the session layer includes full-duplex, half- duplex, and simplex communications. Session layer management also helps to ensure that multiple streams of data stay synchronized with each other, as in the case of multimedia applications like video conferencing, and assists with the prevention of application related data errors.

The session layer is responsible for creating, maintaining, and tearing down the session.

Three modes are offered:

(Full) Duplex: Both hosts can exchange information simultaneously, independent of each other. Half Duplex: Hosts can exchange information, but only one host at a time. Simplex: Only one host can send information to its peer. Information travels in one direction only.

Another aspect of performance that is worthy of some attention is the mode of operation of the network or connection. Obviously, whenever we connect together device A and device B, there must be some way for A to send to B and B to send to
A.Many people don't realize, however, that networking technologies can differ in terms of how these two directions of communication are handled. Depending on how the network is set up, and

the characteristics of the technologies used, performance may be improved through the selection of performance-enhancing modes.
Basic Communication Modes of Operation

Let's begin with a look at the three basic modes of operation that can exist for any network connection, communications channel, or interface.
Simplex Operation

In simplex operation, a network cable or communications channel can only send information in one direction; it's a "one-way street". This may seem counter-intuitive: what's the point of communications that only travel in one direction? In fact, there are at least two different places where simplex operation is encountered in modern networking.

The first is when two distinct channels are used for communication: one transmits from A to B and the other from B to
A.This is surprisingly common, even though not always obvious. For example, most if not all fiber optic communication is simplex, using one strand to send data in each direction. But this may not be obvious if the pair of fiber strands are combined into one cable.

Simplex operation is also used in special types of technologies, especially ones that are asymmetric. For example, one type of satellite Internet access sends data over the satellite only for downloads, while a regular dial-up modem is used for upload to the service provider. In this case, both the satellite link and the dial-up connection are operating in a simplex mode.
Half-Duplex Operation

Technologies that employ half-duplex operation are capable of sending information in both directions between two nodes, but only one direction or the other can be utilized at a time. This is a fairly common mode of operation when there is only a single network medium (cable, radio frequency and so forth) between devices.

While this term is often used to describe the behavior of a pair of devices, it can more generally refer to any number of connected devices that take turns transmitting. For example, in conventional Ethernet networks, any device can transmit, but only one may do so at a time. For this reason, regular (unswitched) Ethernet networks are often said to be "half-duplex", even though it may seem strange to describe a LAN that way.

Full-Duplex Operation
In full-duplex operation, a connection between two devices is capable of sending data in both directions simultaneously. Full-duplex channels can be constructed either as a pair of simplex links (as described above) or using one channel designed to permit bidirectional simultaneous transmissions. A full-duplex link can only connect two devices, so many such links are required if multiple devices are to be connected together.

Note that the term "full-duplex" is somewhat redundant; "duplex" would suffice, but everyone still says "full-duplex" (likely, to differentiate this mode from half-duplex).

For a listing of protocols associated with Layer 5 of the OSI model, see below:

ADSP - AppleTalk Data Stream Protocol
ASP - AppleTalk Session Protocol
H.245 - Call Control Protocol for Multimedia Communication ISO-SP
OSI session-layer protocol (X.225, ISO 8327)
iSNS - Internet Storage Name Service

The following are incorrect answers:

Synchronous and Asynchronous are not session layer modes.

Half simplex does not exist. By definition, simplex means that information travels one way only, so half-simplex is a oxymoron.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 5603-5636). Auerbach Publications. Kindle Edition.
http://www.tcpipguide.com/free/t_SimplexFullDuplexandHalfDuplexOperation.htm
http://www.wisegeek.com/what-is-a-session-layer.htm

QUESTION 462
Which of the following types of Intrusion Detection Systems uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host?

A. Network-based ID systems.
B. Anomaly Detection.
C. Host-based ID systems.
D. Signature Analysis.

Correct Answer: B
Explanation:
There are two basic IDS analysis methods: pattern matching (also called signature analysis) and anomaly detection.

Anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host.
Anomalies may include but are not limited to:

Multiple failed log-on attempts
Users logging in at strange hours
Unexplained changes to system clocks
Unusual error messages

The following are incorrect answers:
Network-based ID Systems (NIDS) are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.

Host-based ID Systems (HIDS) is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.

Signature Analysis Some of the first IDS products used signature analysis as their detection

method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. For example, an attacker manipulating an FTP server may use a tool that sends a specially constructed packet. If that particular packet pattern is known, it can be represented in the form of a signature that IDS can then compare to incoming packets. Pattern-based IDS will have a database of hundreds, if not thousands, of signatures that are compared to traffic streams. As new attack signatures are produced, the system is updated, much like antivirus solutions. There are drawbacks to pattern-based IDS. Most importantly, signatures can only exist for known attacks. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS. Additionally, if an attacker knows that the IDS is present, he or she can alter his or her methods to avoid detection. Changing packets and data streams, even slightly, from known signatures can cause an IDS to miss the attack. As with some antivirus systems, the IDS is only as good as the latest signature database on the system.

For additional information on Intrusion Detection Systems -
http://en.wikipedia.org/wiki/Intrusion_detection_system

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3623-3625, 3649-3654, 3666-3686). Auerbach Publications. Kindle Edition.

QUESTION 463
Which of the following best describes signature-based detection?

A. Compare source code, looking for events or sets of events that could cause damage to a system or network.
B. Compare system activity for the behaviour patterns of new attacks.
C. Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.
D. Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.

Correct Answer: C
Explanation:
Misuse detectors compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection."

The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.

Reference:
Old Document:
BACE, Rebecca & MELL, Peter, NIST Special Publication 800-31 on Intrusion Detection Systems, Page 16.
The publication above has been replaced by 800-94 on page 2-4
The Updated URL is: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf