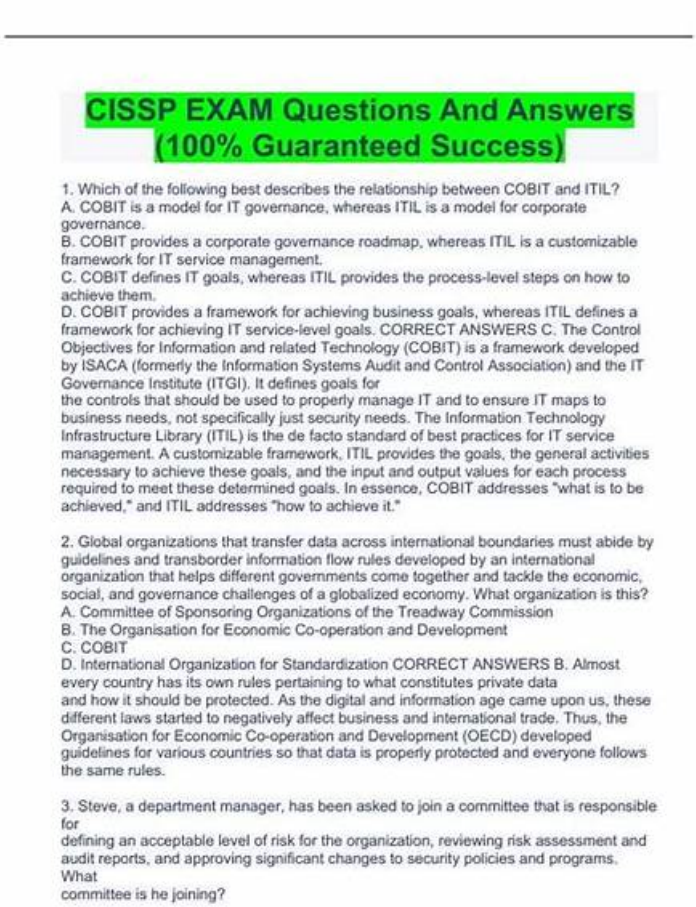
Pass Guaranteed Quiz ISC CISSP - First-grade Exam Certified Information Systems Security Professional (CISSP) Questions



CISSP EXAM Questions And Answers (100% Guaranteed Success)

1. Which of the following best describes the relationship between COBIT and ITIL?
A. COBIT is a model for IT governance, whereas ITIL is a model for corporate governance.
B. COBIT provides a corporate governance roadmap, whereas ITIL is a customizable framework for IT service management.
C. COBIT defines IT goals, whereas ITIL provides the process-level steps on how to achieve them.
D. COBIT provides a framework for achieving business goals, whereas ITIL defines a framework for achieving IT service-level goals. CORRECT ANSWERS C. The Control Objectives for Information and related Technology (COBIT) is a framework developed by ISACA (formerly the Information Systems Audit and Control Association) and the IT Governance Institute (ITGI). It defines goals for
the controls that should be used to properly manage IT and to ensure IT maps to business needs, not specifically just security needs. The Information Technology Infrastructure Library (ITIL) is the de facto standard of best practices for IT service management. A customizable framework, ITIL provides the goals, the general activities necessary to achieve these goals, and the input and output values for each process required to meet these determined goals. In essence, COBIT addresses "what is to be achieved," and ITIL addresses "how to achieve it."

2. Global organizations that transfer data across international boundaries must abide by guidelines and transborder information flow rules developed by an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. What organization is this?
A. Committee of Sponsoring Organizations of the Treadway Commission
B. The Organisation for Economic Co-operation and Development
C. COBIT
D. International Organization for Standardization CORRECT ANSWERS B. Almost every country has its own rules pertaining to what constitutes private data
and how it should be protected. As the digital and information age came upon us, these different laws started to negatively affect business and international trade. Thus, the Organisation for Economic Co-operation and Development (OECD) developed guidelines for various countries so that data is properly protected and everyone follows the same rules.

3. Steve, a department manager, has been asked to join a committee that is responsible for
defining an acceptable level of risk for the organization, reviewing risk assessment and audit reports, and approving significant changes to security policies and programs. What
committee is he joining?

P.S. Free 2026 ISC CISSP dumps are available on Google Drive shared by PDF4Test: https://drive.google.com/open?id=1Q3pX7Y3g0gG-WEpZDrP94SID6JdxnBpg

If you are willing to clear exam successfully, you need to not only read books and study materials but also purchase ISC CISSP reliable exam cram for well-directed review which will make you half the work with double results. You can find three versions for each exam: PDF version, Software version and APP version. You can choose one or more versions of CISSP Reliable Exam Cram based on your studying methods and habits.

Preparing for the CISSP certification exam requires a significant amount of time and effort. Candidates are required to have a minimum of five years of professional experience in the field of information security to be eligible to take the exam. In addition, candidates are required to pass a rigorous exam that tests their knowledge and skills across multiple domains. CISSP Exam is challenging, and candidates must be prepared to dedicate a significant amount of time and effort to prepare for it.

>> Exam CISSP Questions <<

PDF4Test CISSP Exam Questions are Verified by Subject Matter Experts

This is useful for Certified Information Systems Security Professional (CISSP) (CISSP) applicants who want to practice at any moment and do not want to sit in front of a computer all day. Candidates can choose the ISC CISSP pdf questions format that is most convenient for them. Candidates can download and print the CISSP PDF Questions and practice for the CISSP exam on their smartphones, laptops, or tablets at any time, which gives it an advantage over others.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q1105-Q1110):

NEW QUESTION # 1105
Which Identity and Access Management (IAM) process can be used to maintain the principle of least privilege?

- A. user access review
- B. identity provisioning
- C. multi-factor authentication (MFA)
- D. access recovery

Answer: A

Explanation:
User access reviews are a key Identity and Access Management (IAM) process that helps maintain the principle of least privilege. The principle of least privilege states that users should only have access to the resources and permissions necessary to perform their job functions. Over time, users may accumulate unnecessary or excessive permissions due to changes in roles, job functions, or projects. Regular user access reviews help ensure that users only retain the appropriate level of access and remove any unnecessary or outdated permissions.
During user access reviews:
Access levels and permissions are audited to ensure they are in line with the user's current role and responsibilities.
Unnecessary access or permissions that go beyond what is required for the user's duties can be revoked.
This process ensures that employees are not granted more privileges than needed, helping to reduce the risk of accidental or malicious misuse of privileges.

NEW QUESTION # 1106
Who vouches for the binding between the data items in a digital certificate?

- A. Issuing authority
- B. Registration authority
- C. Vouching authority
- D. Certification authority

Answer: D

Explanation:
A certification authority (CA) is an entity that issues digital certificates
(especially X.509 certificates) and vouches for the binding between the data items in a certificate. An issuing authority could be considered a correct answer, but not the best answer, since it is too generic.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION # 1107
Controls are implemented to:

- A. eliminate risk and eliminate the potential for loss
- B. mitigate risk and eliminate the potential for loss
- C. eliminate risk and reduce the potential for loss
- D. mitigate risk and reduce the potential for loss

Answer: D

Explanation:
Controls are implemented to mitigate risk and reduce the potential for loss.
Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful

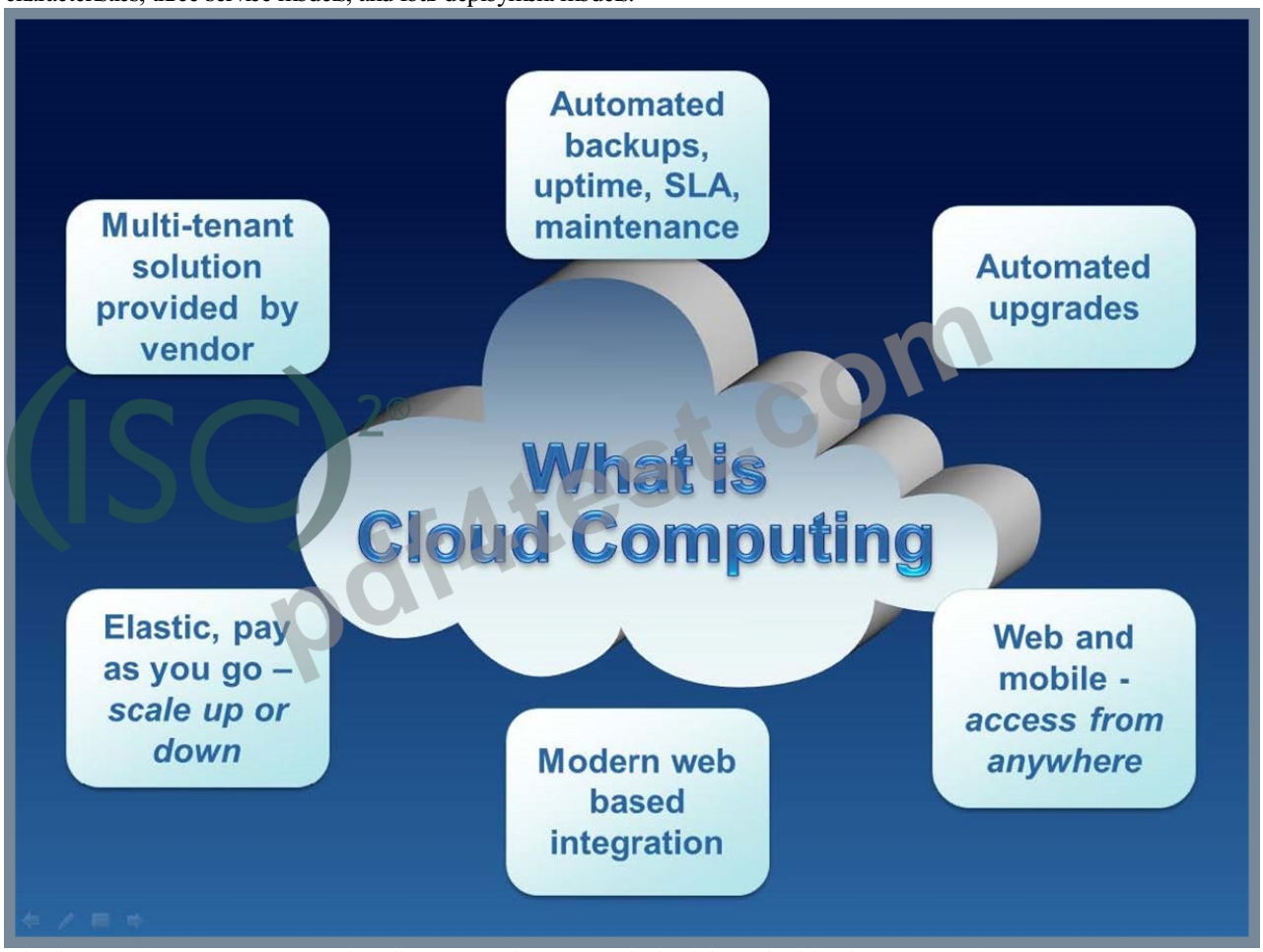
occurrences; corrective controls are used to restore systems that are victims of harmful attacks.
It is not feasible and possible to eliminate all risks and the potential for loss as risk/threats are constantly changing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the
Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32

NEW QUESTION # 1108
Which of the following cloud computing service model provides a way to rent operating systems, storage and network capacity over the Internet?

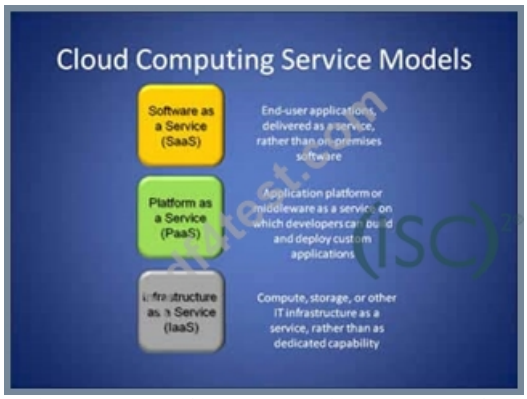
- A. Data as a service
- B. Software as a service
- C. Infrastructure as a service
- D. Platform as a service

Answer: D

Explanation:
Platform as a Service (PaaS) is a way to rent operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.
For your exam you should know below information about Cloud Computing:
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.



Cloud Computing Image Reference http://osarena.net/wp-content/uploads/2013/04/cloud-computing3.jpg
Cloud computing service models: Cloud computing service models Image Reference
http://www.esri.com/news/arcwatch/0110/graphics/feature2.jpg



Software as a Service (SaaS) Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution. Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network based access to a single copy of an application created specifically for SaaS distribution and use.

Benefits of the SaaS model include: easier administration automatic updates and patch management compatibility: All users will have the same version of software. easier collaboration, for the same reason global accessibility.

Platform as a Service (PaaS)

Platform as a Service (PaaS) is a way to rent operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Cloud providers deliver a computing platform,which can include an operating system, database, and web server as a holistic execution environment. Where IaaS is the "raw IT network," PaaS is the software environment that runs on top of the IT network.

Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts. On the downside, PaaS involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

Infrastructure as a Service (IaaS)

Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Characteristics and components of IaaS include:

Utility computing service and billing model. Automation of administrative tasks.

Dynamic scaling. Desktop virtualization. Policy-based services. Internet connectivity.

Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).

The following answers are incorrect:

Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.

Software as a service - Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models.

Infrastructure as a service - Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

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

CISA review manual 2014 page number 102 Official ISC2 guide to CISSP 3rd edition Page number 689

http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS

http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

NEW QUESTION # 1109
Which of the following vulnerabilities can be BEST detected using automated analysis?

- A. Multi-step process attack vulnerabilities
- B. Valid cross-site request forgery (CSRF) vulnerabilities
- C. Typical source code vulnerabilities
- D. Business logic flaw vulnerabilities

Answer: C

Explanation:
The type of vulnerabilities that can be best detected using automated analysis is typical source code vulnerabilities. Automated analysis is a technique that uses automated tools or software to analyze or test a system or an application, and to identify or report any errors, defects, or vulnerabilities. Automated analysis can be performed at different stages of the system or application development life cycle, such as design, coding, testing, or deployment. Typical source code vulnerabilities are the vulnerabilities that are common or frequent in the source code of a system or an application, and that are caused by coding errors, mistakes, or bad practices, such as buffer overflow, integer overflow, memory leak, or hard-coded credentials. Typical source code vulnerabilities can be best detected using automated analysis, as they can be easily scanned, checked, or verified by the automated tools or software, and they can be reported or corrected in a timely and efficient manner. Valid cross-site request forgery (CSRF) vulnerabilities, multi-step process attack vulnerabilities, or business logic flaw vulnerabilities are not the types of vulnerabilities that can be best detected using automated analysis, as they are more complex or specific in the system or the application, and they may require human intervention or judgment to analyze or test. Valid CSRF vulnerabilities are the vulnerabilities that allow an attacker to force a web browser to perform an unwanted or malicious action on a web server, such as transferring funds, changing passwords, or updating profiles, by exploiting the trust between the web browser and the web server. Multi-step process attack vulnerabilities are the vulnerabilities that allow an attacker to compromise a system or an application that involves multiple steps or stages, such as authentication, authorization, or transaction, by exploiting the weaknesses or gaps in each step or stage.
Business logic flaw vulnerabilities are the vulnerabilities that allow an attacker to manipulate or bypass the business rules or the logic of a system or an application, such as workflows, validations, or calculations, by exploiting the flaws or errors in the design or the implementation of the system or the application.
References: Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 21: Software Development Security, page 2010.

NEW QUESTION # 1110
.....

Download " CISSP " for free by simply searching on ➽ www.practicevce.com □ □CISSP Latest Cram Materials

- Valid CISSP Mock Test □ Test CISSP Questions □ CISSP Latest Cram Materials □ Copy URL ✔ www.pdfvce.com □✔□ open and search for ➽ CISSP □ to download for free □CISSP Actual Test
- Real CISSP Questions - Remove Your Exam Fear □ Search for ☀ CISSP □☀□ and download it for free immediately on ☀ www.examdiscuss.com □☀□ □CISSP Reliable Dump
- umarxqqp220545.bloggactif.com, lilywnws347581.azuria-wiki.com, thebookmarkplaza.com, www.stes.tyc.edu.tw, deaconjtqw036537.techionblog.com, myaqbyg831104.creacionblog.com, heiditrlm072618.oneworldwiki.com, bookmarksoflife.com, friendlybookmark.com, roxanndkkl049359.bloguerosa.com, Disposable vapes

2026 Latest PDF4Test CISSP PDF Dumps and CISSP Exam Engine Free Share: https://drive.google.com/open?id=1Q3pX7Y3g0gG-WEpZDrP94SID6JdxnBpg