**Pre-Assessment Quiz**

**1.** What type of solutions enable enterprises or individuals to store their data and computer

files on the Internet using a storage service provider rather than storing the data locally on a

physical disk, such as a hard drive or tape backup?

**A.** Online backups

**B.** Cloud backup solutions

**C.** Removable hard drives

**D.** Masking

**2.** When using an Infrastructure as a Service (IaaS) solution, what is the key benefit for the

customer?

**A.** Scalability

**B.** Metered service

**C.** Energy and cooling efficiencies

**D.** Transfer of ownership cost

**3.** focuses on security and encryption to prevent unauthorized copying and

limitations on distribution to only those who pay.

**A.** Digital rights management (DRM)

**B.** Enterprise digital rights management

**C.** Bit splitting

**D.** Degaussing

**4.** Which of the following represents the correct set of four cloud deployment models?

**A.** Public, Private, Joint and Community

**B.** Public, Private, Hybrid, and Community

**C.** Public, Internet, Hybrid, and Community

**D.** External, Private, Hybrid, and Community

**5.** What is a special mathematical code that allows encryption hardware/software to encode

and then decipher an encrypted message called?

**A.** PKI

**B.** Encryption key

**C.** Public key

**D.** Masking

**6.** Which of the following lists the correct six components of the STRIDE threat model?

**A.** Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and

Elevation of Privilege

**B.** Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and

Social Engineering Elasticity

**C.** Spoofing, Tampering, Repudiation, Information Disclosure, Distributed Denial of Service,

and Elevation of Privilege

**D.** Spoofing, Tampering, Nonrepudiation, Information Disclosure, Denial of Service, and

Elevation of Privilege

**7.** What is the term for the assurance that a specific author actually created and sent a specific

item to a specific recipient, and that the message was successfully received?

**A.** PKI

**B.** DLP

**C.** Nonrepudiation

**D.** Bit splitting

**8.** What is the correct term for the process of deliberately destroying the encryption keys used

to encrypt data?

**A.** Poor key management

**B.** PKI

**C.** Obfuscation

**D.** Crypto-shredding

**9.** In a federated environment, who is the relying party, and what do they do?

**A.** The relying party is the service provider and they would consume the tokens generated

by the identity provider.

**B.** The relying party is the service provider and they would consume the tokens generated

by the customer.

**C.** The relying party is the customer and they would consume the tokens generated by the

identity provider.

**D.** The relying party is the identity provider and they would consume the tokens generated

by the service provider.

**10.** What is the process of replacing sensitive data with unique identification symbols that

retain all the essential information about the data without compromising its security?

**A.** Randomization

**B.** Elasticity

**C.** Obfuscation

**D.** Tokenization

**11.** Which of the following data storage types are associated or used with Platform as a Service

(PaaS)?

**A.** Databases and Big Data

**B.** SaaS application

**C.** Tabular

**D.** Raw and block

**12.** What is the term used for software technology that encapsulates application software from

the underlying operating system on which it is executed?

**A.** Hypervisor

**B.** Application virtualization

**C.** VMWare

**D.** SaaS

**13.** Which of the following represents the legislation enacted to protect shareholders and the

public from enterprise accounting errors and fraudulent practices?

**A.** PCI

**B.** Gramm-Leach-Bliley Act (GLBA)

**C.** Sarbanes-Oxley Act (SOX)

**D.** HIPAA

**14.** What is a device called that can safely store and manage encryption keys and is used in

servers, data transmission, and log files?

**A.** Private key

**B.** Hardware security module (HSM)

**C.** Public key

**D.** Trusted Operating System Module (TOS)

**15.** What is a type of cloud infrastructure that is provisioned for open use by the general public

and is owned, managed, and operated by a business, academic, or government organization

and exists on the premises of the cloud provider called?

**A.** Private cloud

**B.** Public cloud

**C.** Hybrid cloud

**D.** Personal cloud

**16.** When using transparent encryption of a database, where does the encryption engine reside?

**A.** Within the database application itself

**B.** At the application using the database

**C.** On the instances attached to the volume

**D.** In a key management system

**17.** What is a type of assessment called that employs a set of methods, principles, or rules for

assessing risk based on non-numerical categories or levels?

**A.** Quantitative assessment

**B.** Qualitative assessment

**C.** Hybrid assessment

**D.** SOC 2

**18.** What best describes the Cloud Security Alliance Cloud Controls Matrix?

**A.** A set of regulatory requirements for cloud service providers

**B.** A set of software development life cycle requirements for cloud service providers

**C.** A security controls framework that provides mapping/cross relationships with the main

industry-accepted security standards, regulations, and controls frameworks such as the

ISO 27001/27002, ISACA’s COBIT, and PCI-DSS

**D.** An inventory of cloud security controls that are arranged into separate security domains

**19.** When a conflict of laws occurs, determines the jurisdiction in which

the dispute will be heard.

**A.** Tort law

**B.** Doctrine of Proper Law

**C.** Common law

**D.** Criminal law

**20.** Which one of the following is the *most* important security consideration when selecting a

new computer facility?

**A.** Local law enforcement response times

**B.** Location adjacent to competitor’s facilities

**C.** Aircraft flight paths

**D.** Utility infrastructure

**21.** Which of the following is *always* safe to use in the disposal of electronic records within a

cloud environment?

**A.** Physical destruction

**B.** Overwriting

**C.** Encryption

**D.** Degaussing

**22.** Which of the following describes a SYN flood attack?

**A.** Rapid transmission of Internet Relay Chat (IRC) messages

**B.** Creating a high number of partially open TCP connections

**C.** Disabling the Domain Name Service (DNS) server

**D.** Excessive list linking of users and files

**23.** Which of the following is an example of a form of cloud storage that applies to storing an

individual’s mobile device data in the cloud and providing the individual with access to the

data from anywhere?

**A.** Raw storage

**B.** Flash storage

**C.** Obfuscation archiving

**D.** Mobile cloud storage

**24.** Which of the following terms best describes a distributed model where software applications

are hosted by a vendor or cloud service provider and made available to customers over

network resources?

**A.** Infrastructure as a Service (IaaS)

**B.** Public cloud

**C.** Software as a Service (SaaS)

**D.** Private cloud

**25.** Which of the following is a federal law enacted in the United States to control the way that

financial institutions deal with private information of individuals?

**A.** PCI

**B.** ISO/IEC

**C.** Gramm-Leach-Bliley Act (GLBA)

**D.** Consumer Protection Act

**26.** The typical function of Secure Sockets Layer (SSL) in securing Wireless Application Protocol

(WAP) is to protect transmissions that exist:

**A.** Between the WAP gateway and the wireless endpoint device

**B.** Between the web server and the WAP gateway

**C.** From the web server to the wireless endpoint device

**D.** Between the wireless device and the base station

**27.** What is an accounting report on controls at a service organization that replaces older

SAS70 type reports?

**A.** SOC 1

**B.** SSAE16

**C.** GAAP

**D.** SOC 2

**28.** What is a company that purchases hosting services from a cloud server hosting or cloud

computing provider who then resells to its own customers?

**A.** Cloud broker

**B.** Cloud computing reseller

**C.** Cloud proxy

**D.** VAR

**29.** What is a type of computing comparable to grid computing that relies on sharing computing

resources rather than having local servers or personal devices to handle applications?

**A.** Server hosting

**B.** Legacy computing

**C.** Cloud computing

**D.** Intranet

**30.** What is a set of technologies designed to analyze application source code and binaries for

coding and design conditions that are indicative of security and vulnerabilities?

**A.** Dynamic application security testing (DAST)

**B.** Static application security testing (SAST)

**C.** Secure coding

**D.** OWASP

**Answers to Pre-Assessment Quiz**

**1.** B. Cloud backup solutions enable enterprises to store their data and computer files on

the Internet using a storage service rather than storing data locally on a hard disk or tape

backup. This has the added benefit of providing access to data should the primary business

location be damaged in some way that prevents accessing or restoring data locally due to

damaged infrastructure or equipment. Online backups and removable hard drives are other

options but do not by default supply the customer with ubiquitous access. Masking is a

technology used to partially conceal sensitive data.

**2.** D. The primary benefit to the customer of using Infrastructure as a Service (IaaS) is the

transfer of cost of ownership. In a cloud environment, the customer uses and is billed only

for what they use as opposed to the full cost of implementation, saving them a significant

amount in terms of cost of ownership. While scalability, metered service, and energy and

cooling efficiencies are a part of the benefit of a cloud computing environment, they are not

the primary benefit or business driver behind IaaS adoption.

**3.** A. Digital rights management (DRM) was designed to focus on security and encryption as

a means of preventing unauthorized copying and limitations on distribution of content to

only those authorized (purchasers). Enterprise digital rights management, also known as

information rights management (IRM), is a subset of DRM and typically refers to businessto-

business securing of information rights. Bit splitting is a method of hiding information

across multiple geographical boundaries, and degaussing is a method of deleting data permanently

from magnetic media.

**4.** B. The only correct answer for this is Public, Private, Hybrid, and Community. Joint, Internet,

and External are not cloud models.

**5.** B. An encryption key is just that: a key used to encrypt and decrypt information. It is

mathematical code that supports either hardware- or software-based encryption used to

encode or decode information.

**6.** A. The letters in STRIDE threat model represent **S**poofing of identity, **T**ampering with

data, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege.

The other options are simply mixed up or incorrect versions of the same.

**7.** C. Nonrepudiation means that a specific author or user cannot refute or repudiate that he

or she created and/or sent a message and the receiver of the data or message cannot deny

they received it.

**8.** D. The act of crypto-shredding means destroying the key that was initially used to encrypt

the data, thereby making it forever unrecoverable.

**9.** A. The identity provider would hold all of the identities and generate a token for known

users. The relying party (RP) would be the service provider and would consume the tokens.

All other answers are incorrect.

**10.** D. Replacing sensitive data with unique identification symbols is known as tokenization,

a simple and only somewhat effective way of hiding or concealing sensitive data with the

**xxx** Answers to Assessment Test

replacement of unique identification symbols. It is not considered as strong as encryption

but can be effective in keeping prying eyes off of sensitive information. While randomization

and obfuscation are also means of concealing information, they are done quite

differently.

**11.** A. PaaS uses databases and Big Data storage types.

**12.** B. Application virtualization encapsulates application software from the underlying operating

system on which it is executed.

**13.** C. The Sarbanes-Oxley Act (SOX) was enacted in response to the 2000 accounting scandal

that caused the bankruptcy of Enron. At that time, top executives laid the claim that they

were unaware of the accounting practices that led to the company’s demise. SOX not only

forces executives to oversee all accounting practices, but holds them accountable should

such activity occur again.

**14.** B. A hardware security module is a device that can safely store and manage encryption

keys. These can be used in servers, workstations, and so on. Once common type is called

the Trusted Platform Module (TPM) and can be found on enterprise workstations and

laptops. There is no such term as a trusted operating system, and public and private keys

are terms used with PKI.

**15.** B. This is the very definition of public cloud computing.

**16.** A. In transparent encryption, the encryption key for a database is stored in the boot record

of the database itself.

**17.** B. A qualitative assessment is a set of methods or rules for assessing risk based on nonmathematical

or categories or levels. One that uses those mathematical categories or levels

is called a quantitative assessment. There is no such thing as a hybrid assessment, and an

SOC 2 is an accounting report regarding control effectiveness.

**18.** C. The CCM cross-references many industry standards, laws, and guidelines.

**19.** B. The Doctrine of Proper Law is used when a dispute occurs over which jurisdiction will

hear a case. Tort law refers to civil liability suits. Common law refers to laws regarding

marriage, and criminal law refers to violations of state or federal criminal code.

**20.** D. Of the answers given, option D is the most important. It is vital that any datacenter

facility be close to sound facility resources such as power, water, and connectivity.

**21.** C. Encryption can always be used in a cloud environment, but physical destruction, overwriting,

and degaussing may not be available due to access and physical separation factors.

**22.** B. A SYN flood is where a TCP connection attempt is made and then cut short just prior to

completion, thereby leaving a server waiting for a response. If enough of these connection

attempts are made, a “flood” occurs, causing the end unit to consume resources to the point

that either services and/or the system itself become unavailable for use. The other options

have no connection with a flood of any kind.

Answers to Assessment Test **xxxi**

**23.** D. Mobile cloud storage is defi ned as a form of cloud storage that applies to storing an individual’s

mobile device data in the cloud and providing the individual with access to the data

from anywhere.

**24.** C. This is the defi nition of the Software as a Service (SaaS) service model. Public and private

are cloud deployment models, and Infrastructure as a Service (IaaS) does not provide

applications of any type.

**25.** C. The Gramm-Leach-Bliley Act targets U.S. fi nancial institutions and requires them to

deal specifi cally with protecting account holders’ private information. PCI refers to credit

card processing requirements, ISO/IEC is a standards organization, and the Consumer Protection

Act, while providing oversight for the protection of consumer private information, is

limited in scope.

**26.** C. The purpose of SSL is to encrypt the communication channel between two end points.

In this example, it is the end user and the server.

**27.** A. The correct answer is the SOC 1 report, which is designed to assess the controls primarily

revolving around fi nancial reporting, formerly found in the SAS 70. The SOC 2 is a

report that provides information related to one or more of the AICPA fi ve security

principles.

**28.** B. The cloud computing reseller purchases hosting services and then resells them.

**29.** C. Cloud computing is built on the model of grid computing whereby resources can

be pooled and shared rather than having local devices do all the compute and storage

functions.

**30.** B. Static application security testing (SAST) differs from dynamic application security

testing (DAST) in that it looks at source code and binaries to see if it can detect problems

before the code is loaded into memory and run.