**Review Questions CHAPTER 2**

**1.** Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

**A.** Full inventory

**B.** Usefulness

**C.** Value

**D.** Criticality

**2.** The BIA can be used to provide information about all the following, except:

**A.** Risk analysis

**B.** Secure acquisition

**C.** BC/DR planning

**D.** Selection of security controls

**3.** In which cloud service model is the customer required to maintain the OS?

**A.** CaaS

**B.** SaaS

**C.** PaaS

**D.** IaaS

**4.** In which cloud service model is the customer required to maintain and update only the

applications?

**A.** CaaS

**B.** SaaS

**C.** PaaS

**D.** IaaS

**5.** In which cloud service model is the customer only responsible for the data?

**A.** CaaS

**B.** SaaS

**C.** PaaS

**D.** IaaS

**6.** The cloud customer and provider negotiate their respective responsibilities and rights regarding

the capabilities and data of the cloud service. Where is the eventual agreement codified?

**A.** RMF

**B.** Contract

**C.** MOU

**D.** BIA

**7.** In attempting to provide a layered defense, the security practitioner should convince senior

management to include security controls of which type?

**A.** Technological

**B.** Physical

**C.** Administrative

**D.** All of the above

**8.** Which of the following is considered an administrative control?

**A.** Access control process

**B.** Keystroke logging

**C.** Door locks

**D.** Biometric authentication

**9.** Which of the following is considered a technological control?

**A.** Firewall software

**B.** Fireproof safe

**C.** Fire extinguisher

**D.** Firing personnel

**10.** Which of the following is considered a physical control?

**A.** Carpets

**B.** Ceilings

**C.** Doors

**D.** Fences

**11.** In a cloud environment, encryption should be used for all the following, except:

**A.** Long-term storage of data

**B.** Near-term storage of virtualized images

**C.** Secure sessions/VPN

**D.** Profile formatting

**12.** The process of hardening a device should include all the following, except:

**A.** Improve default accounts

**B.** Close unused ports

**C.** Delete unnecessary services

**D.** Strictly control administrator access

**13.** The process of hardening a device should include which of the following?

**A.** Encrypting the OS

**B.** Updating and patching the system

**C.** Using video cameras

**D.** Performing thorough personnel background checks

**14.** What is an experimental technology that is intended to create the possibility of processing

encrypted data without having to decrypt it first?

**A.** Homomorphic

**B.** Polyinstantiation

**C.** Quantum-state

**D.** Gastronomic

**15.** Risk appetite for an organization is determined by which of the following?

**A.** Appetite evaluation

**B.** Senior management

**C.** Legislative mandates

**D.** Contractual agreement

**16.** What is the risk left over after controls and countermeasures are put in place?

**A.** Null

**B.** High

**C.** Residual

**D.** Pertinent

**17.** All the following are ways of addressing risk, except:

**A.** Acceptance

**B.** Reversal

**C.** Mitigation

**D.** Transfer

**18.** To protect data on user devices in a BYOD environment, the organization should consider

requiring all the following, except:

**A.** DLP agents

**B.** Local encryption

**C.** Multifactor authentication

**D.** Two-person integrity

**19.** Devices in the cloud datacenter should be secure against attack. All the following are means

of hardening devices, except:

**A.** Using a strong password policy

**B.** Removing default passwords

**C.** Strictly limiting physical access

**D.** Removing all admin accounts

**20.** Which of the following best describes risk?

**A.** Preventable

**B.** Everlasting

**C.** The likelihood that a threat will exploit a vulnerability

**D.** Transient

**Chapter 2: Design Requirements**

**1.** B. When we gather information about business requirements, we need to do a complete

inventory, receive accurate valuation of assets (usually from the owners of those assets), and

assess criticality; this collection of information does not tell us, objectively, how useful an

asset is, however.

**2.** B. The business impact analysis gathers asset valuation information that is beneficial for

risk analysis and selection of security controls (it helps avoid putting the ten-dollar lock on

the five-dollar bicycle), and criticality information that helps in BC/DR planning by letting

the organization understand which systems, data, and personnel are necessary to continuously

maintain. However, it does not aid secure acquisition efforts, since the assets examined

by the BIA have already been acquired.

**3.** D. In IaaS, the service is bare metal, and the customer has to install the OS and the software;

the customer then is responsible for maintaining that OS. In the other models, the

provider installs and maintains the OS.

**4.** C. In PaaS, the provider supplies the hardware, connectivity, and OS; the customer installs

and maintains applications. In IaaS, the customer must also install the OS, and in SaaS, the

provider supplies and maintains the applications.

**5.** B. SaaS is the model in which the customer supplies only the data; in the other models, the

customer also supplies the OS, the application, or both.

**6.** B. The contract codifies the rights and responsibilities of the parties involved upon completion

of negotiation. The RMF aids in risk analysis and design of the environment. An MOU

is shared between parties for a number of possible reasons. The BIA aids in risk assessment,

DC/BR efforts, and selection of security controls.

**7.** D. Layered defense calls for a diverse approach to security.

**8.** A. A process is an administrative control; sometimes, the process includes elements of other

types of controls (in this case, the access control mechanism might be a technical control,

or it might be a physical control), but the process itself is administrative. Keystroke logging

is a technical control (or an attack, if done for malicious purposes, and not for auditing);

door locks are a physical control; and biometric authentication is a technological control.

This is a tricky question.

**9.** A. A firewall is a technological control. The safe and extinguisher are physical controls,

and firing someone is an administrative control.

**312** Appendix A ■ Answers to the Review Questions

**10.** D. Fences are physical controls; carpets and ceilings are architectural features, and a door

is not necessarily a control: the lock on the door would be a physical security control.

Although you might think of a door as a potential answer, the best answer is the fence; the

exam will have questions where more than one answer is correct, and the answer that will

score you points is the one that is *most* correct.

**11.** D. All of these activities should incorporate encryption, except for profile formatting,

which is a made-up term.

**12.** A. We don’t want to improve default accounts—we want to remove them. All the other

options are steps we take to harden devices.

**13.** B. Updating and patching the system helps harden the system. Encrypting the OS is a distractor.

That would make the OS/machine impossible to use. Video cameras are a security

control, but not one used to harden a device. Background checks are good for vetting personnel,

but not for hardening devices.

**14.** A. Homomorphic encryption hopes to achieve that goal; the other options are terms that

have almost nothing to do with encryption.

**15.** B. Senior management decides the risk appetite of the organization.

**16.** C. This is the definition of the term.

**17.** B. Reversal is not a method for handling risk.

**18.** D. Although all the other options are ways to harden a mobile device, two-person integrity

is a concept that has nothing to do with the topic, and, if implemented, would require

everyone in your organization to walk around in pairs while using their mobile devices.

**19.** D. Although the rest of the options are good tactics for securing devices, we can’t remove

all admin accounts; the device will need to be administered at some point, and that account

needs to be there.

**20.** C. Option C is the definition of risk—and risk is never preventable: it can be obviated,

attenuated, reduced, and minimized, but never completely prevented. A risk may be everlasting

or transient, indicating that risk itself is not limited to being either.