Chapter 5 Operations Review Questions PART I

**1.** What is the lowest tier of datacenter redundancy, according to the Uptime Institute?

**A.** 1

**B.** V

**C.** C

**D.** 4

**2.** What is the amount of fuel that should be on hand to power generators for backup datacenter

power, in all tiers, according to the Uptime Institute?

**A.** 1

**B.** 1,000 gallons

**C.** 12 hours

**D.** As much as needed to ensure all systems may be gracefully shut down and data

securely stored

**3.** Which of the following is *not* one of the three types of training?

**A.** Integral

**B.** Initial

**C.** Recurring

**D.** Refresher

**4.** Which of the following is part of the STRIDE model?

**A.** Repudiation

**B.** Redundancy

**C.** Resiliency

**D.** Rijndael

**5.** Which of the following is *not* part of the STRIDE model?

**A.** Spoofing

**B.** Tampering

**C.** Resiliency

**D.** Information disclosure

**6.** Which of the following is *not* a feature of SAST?

**A.** Source code review

**B.** Team-building efforts

**C.** “White-box” testing

**D.** Highly skilled, often expensive outside consultants

**7.** Which of the following is *not* a feature of DAST?

**A.** Testing in runtime

**B.** User teams performing executable testing

**C.** “Black-box” testing

**D.** Binary inspection

**8.** Which of the following is *not* a feature of a secure KVM component?

**A.** Keystroke logging

**B.** Sealed exterior case

**C.** Welded chipsets

**D.** Push-button selectors

**9.** What type of redundancy can we expect to find in a datacenter of any tier?

**A.** All operational components

**B.** All infrastructure

**C.** Emergency egress

**D.** Full power capabilities

**10.** What should be the primary focus of datacenter redundancy and contingency planning?

**A.** Critical path/operations

**B.** Health and human safety

**C.** Infrastructure supporting the production environment

**D.** Power and HVAC

**11.** Which of the following techniques for ensuring cloud datacenter storage resiliency uses parity

bits and disk striping?

**A.** Cloud-bursting

**B.** RAID

**C.** Data dispersion

**D.** SAN

**12.** Which resiliency technique attenuates the possible loss of functional capabilities during

contingency operations?

**A.** Cross-training

**B.** Metered usage

**C.** Proper placement of HVAC temperature measurements tools

**D.** Raised floors

**13.** Which of the following has *not* been attributed as the cause of lost capabilities due to DoS?

**A.** Hackers

**B.** Construction equipment

**C.** Changing regulatory motif

**D.** Squirrels

**14.** Which of the following aids in the ability to demonstrate due diligence efforts?

**A.** Redundant power lines

**B.** HVAC placement

**C.** Security training documentation

**D.** Bollards

**15.** What is often a major challenge to getting both redundant power and communications utility

connections?

**A.** Expense

**B.** Carrying medium

**C.** Personnel deployment

**D.** Location of many datacenters

**16.** Which of the following is *not* an aspect of physical security that ought to be considered in

the planning and design of a cloud datacenter facility?

**A.** Perimeter

**B.** Vehicular approach/traffic

**C.** Fire suppression

**D.** Elevation of dropped ceilings

**17.** The Brewer-Nash security model is also known as which of the following?

**A.** MAC

**B.** The Chinese Wall model

**C.** Preventive measures

**D.** RBAC

**18.** Which kind of hypervisor would malicious actors prefer to attack, ostensibly because it

offers a greater attack surface?

**A.** Cat IV

**B.** Type II

**C.** Bare metal

**D.** Converged

**19.** Which of the following techniques for ensuring cloud datacenter storage resiliency uses

encrypted chunks of data?

**A.** Cloud-bursting

**B.** RAID

**C.** Data dispersion

**D.** SAN

**20.** Security training should *not* be:

**A.** Documented

**B.** Internal

**C.** A means to foster a non-adversarial relationship between the security office and operations

personnel

**D.** Boring

Review Questions Chapter 5 Operations PART II

**1.** Which form of BC/DR testing has the most impact on operations?

**A.** Tabletop

**B.** Dry run

**C.** Full test

**D.** Structured test

**2.** Which form of BC/DR testing has the least impact on operations?

**A.** Tabletop

**B.** Dry run

**C.** Full test

**D.** Structured test

**3.** Which characteristic of liquid propane increases its desirability as a fuel for backup

generators?

**A.** Burn rate

**B.** Price

**C.** Does not spoil

**D.** Flavor

**4.** How often should the CMB meet?

**A.** Whenever regulations dictate

**B.** Often enough to address organizational needs and attenuate frustration with delay

**C.** Every week

**D.** Annually

**5.** Adhering to ASHRAE standards for humidity can reduce the possibility of .

**A.** Breach

**B.** Static discharge

**C.** Theft

**D.** Inversion

**6.** A UPS should have enough power to last how long?

**A.** 12 hours

**B.** 10 minutes

**C.** One day

**D.** Long enough for graceful shutdown

**236** Chapter 9 ■ Operations Management

**7.** A generator transfer switch should bring backup power online within what time frame?

**A.** 10 seconds

**B.** Before the recovery point objective is reached

**C.** Before the UPS duration is exceeded

**D.** Three days

**8.** Which characteristic of automated patching makes it attractive?

**A.** Cost

**B.** Speed

**C.** Noise reduction

**D.** Capability to recognize problems quickly

**9.** Which tool can reduce confusion and misunderstanding during a BC/DR response?

**A.** Flashlight

**B.** Controls matrix

**C.** Checklist

**D.** Call tree

**10.** When deciding whether to apply specific updates, it is best to follow , in order to

demonstrate due care.

**A.** Regulations

**B.** Vendor guidance

**C.** Internal policy

**D.** Competitors’ actions

**11.** The CMB should include representations from all of the following offices except:

**A.** Regulators

**B.** IT department

**C.** Security office

**D.** Management

**12.** For performance purposes, OS monitoring should include all of the following except:

**A.** Disk space

**B.** Disk I/O usage

**C.** CPU usage

**D.** Print spooling

**13.** Maintenance mode requires all of these actions except:

**A.** Remove all active production instances

**B.** Initiate enhanced security controls

**C.** Prevent new logins

**D.** Ensure logging continues

**14.** What is one of the reasons a baseline might be changed?

**A.** Numerous change requests

**B.** Power fluctuation

**C.** To reduce redundancy

**D.** Natural disaster

**15.** In addition to battery backup, a UPS can offer which capability?

**A.** Communication redundancy

**B.** Line conditioning

**C.** Breach alert

**D.** Confidentiality

**16.** Deviations from the baseline should be investigated and .

**A.** Documented

**B.** Enforced

**C.** Revealed

**D.** Encouraged

**17.** The baseline should cover which of the following?

**A.** As many systems throughout the organization as possible

**B.** Data breach alerting and reporting

**C.** A process for version control

**D.** All regulatory compliance requirements

**18.** A localized incident or disaster can be addressed in a cost-effective manner by using which

of the following?

**A.** UPS

**B.** Generators

**C.** Joint operating agreements

**D.** Strict adherence to applicable regulations

**19.** Generator fuel storage for a cloud datacenter should last for how long, at a minimum?

**A.** 10 minutes

**B.** Three days

**C.** Indefinitely

**D.** 12 hours

**20.** The BC/DR kit should include all of the following except:

**A.** Flashlight

**B.** Documentation equipment

**C.** Hard drives

**D.** Annotated asset inventory

Answers Chapter 5 Operations Review Questions PART I

**1.** A. There are four tiers of the Uptime Institute's datacenter redundancy rating system, with

1 being the lowest and 4 the highest.

**2.** C. The other answers are distractors.

**3.** A. The three common types of security training are initial, recurring, and refresher.

**4.** A. Repudiation is an element of the STRIDE model; the rest of the answers are not.

**5.** C. Resiliency is not an element of the STRIDE model; all the rest of the answers are.

**6.** B. Team-building has nothing to do with SAST; all the rest of the answers are characteristics

of SAST.

**7.** D. Binary inspection has nothing to do with DAST, and it is not really a term that means

anything in our industry (although it could be interpreted as a type of code review, more

related to SAST); all the rest of the answers are characteristics of DAST.

**8.** A. Keystroke logging is not a characteristic of secure KVM design; in fact, secure KVM

components should attenuate the potential for keystroke logging. All the rest of the answers

are characteristics of secure KVM components.

**9.** C. Emergency egress redundancy is the only aspect of datacenters that can be expected to

be found in datacenters of any tier; the rest of the answers list characteristics that can be

found only in specific tiers.

**10.** B. Regardless of the tier level or purpose of any datacenter, design focus for security should

always consider health and human safety paramount.

**11.** B. Parity bits and disk striping are characteristic of RAID implementations. Cloud-bursting

is a feature of scalable cloud hosting. Data dispersion uses parity bits, but not disk striping;

instead, it uses data chunks and encryption. SAN is a data storage technique, but not

focused on resiliency.

**12.** A. Cross-training offers attenuation of lost contingency capabilities by ensuring personnel

will be able to perform essential tasks, even if they are not primarily assigned to those positions

in a full-time capacity. Metered usage is a benefit for cloud customers associated with

ensuring value for payment, but not resiliency. Proper placement of HVAC temperature

measurement and raised floors both aid in optimizing component performance but are not

practically associated with resiliency. This is a difficult question, and it could be read in

ways that would suggest other correct answers.

**13.** C. Changing regulations should not result in lack of availability. All the other answers have

caused DoS outages.

**14.** C. Security training documentation can be used to show that personnel have received adequate,

pertinent training to a suitable level, which demonstrates due diligence—that is, effort in furtherance

of due care. All the other answers are beneficial to the resiliency and durability of the

datacenter, but they are not methods for demonstrating due diligence. This is a difficult question,

and it could be read in ways that would suggest other correct answers.

**15.** D. The location of many datacenters—rurally situated, distant from metropolitan areas—may

create challenges for finding multiple power utility providers and ISPs, as those areas just aren’t

usually served by multiple vendors. Expense is not usually a concern; economies of scale make

costs acceptable as part of the pricing structure. Personnel deployment doesn’t usually affect

access to either type of connection. The carrying medium has nothing to do with challenges for

finding multiple providers and is not even a common industry term.

**16.** D. The height of dropped ceilings is not a security concern, except in action movies. The

rest of the answers are all aspects of physical security that should be taken into account

when planning and designing a datacenter.

**17.** B. The Brewer-Nash model is also known as the Chinese Wall model.

**18.** B. Type II hypervisors run via the OS on the host machine; this makes them attractive to

attackers, as both the machine and the OS offer potential attack vectors. Cat IV and converged

are not terms associated with hypervisors. Bare-metal hypervisors (Type I) are less

preferable to attackers, as they offer less attack surface.

**19.** C. Data dispersion uses parity bits, data chunks, and encryption. Parity bits and disk striping

are characteristic of RAID implementations. Cloud-bursting is a feature of scalable

cloud hosting. SAN is a data storage technique but not focused on resiliency.

**20.** D. Security training should not be boring; you want attendees to be enthused so that they

pay attention, which enhances recall of the material, elevating security for the organization.

All the other answers are characteristics of good security training.

Answers Chapter 5 Operations Review Questions PART II

**1.** C. The full test will involve every asset in the organization, including all personnel. The

others will have lesser impact, except for D, which is a red herring.

**2.** A. The tabletop testing involves only essential personnel and none of the production assets.

The others will have greater impact, except for D, which is a red herring.

**3.** C. Liquid propane does not spoil, which obviates necessity for continually refreshing and

restocking it and might make it more cost-effective. The burn rate has nothing to do with

its suitability, unless it has some direct bearing on the particular generator the datacenter

owner has chosen. The various relative prices of fuel fluctuate. Flavor is a distractor in this

question and means nothing.

**4.** B. Frustrated employees and managers can increase risk to the organization by implementing

their own, unapproved modifications to the environment. The particular interval

changes from organization to organization.

**5.** B. A datacenter with less than optimum humidity can have a higher static electricity discharge

rate. Humidity has no bearing on breaches or theft, and inversion is a nonsense term

used as a distractor.

**6.** D. The UPS is intended to last only long enough to save production data currently being

processed. The exact quantity of time will depend on many variables and will differ from

one datacenter to the next.

**7.** C. Generator power should be online before battery backups fail. The specific amount of

time will vary between datacenters.

**8.** B. Automated patching is much faster and more efficient than manual patching. It is, however,

not necessarily any less expensive than manual patching. Manual patching is overseen

by administrators, who will recognize problems faster than automated tools. Noise reduction

is not a factor in patch management at all.

**9.** C. Checklists serve as a reliable guide for BC/DR activity and should be straightforward

enough to use that someone not already an expert or trained in BC/DR response could

ostensibly accomplish the necessary tasks. Flashlights and call trees are certainly useful

during BC/DR actions, but not for the purpose of reducing confusion and misunderstanding.

Control matrices are not useful during BC/DR actions.

**10.** B. A datacenter that doesn’t follow vendor guidance might be seen as failing to provide due

care. Regulations, internal policy, and the actions of competitors might all inform the decision

to perform an update and patch, but these are not necessarily directly bearing on due care. This

is a difficult, nuanced question, and all the answers are good, but option B is the best.

**11.** A. Regulators are not involved in an organization’s CMB; all the rest are.

**12.** D. Print spooling is not a metric for system performance; all the rest are.

**13.** B. While the other answers are all steps in moving from normal operations to maintenance

mode, we do not necessarily initiate any enhanced security controls.

**14.** A. If the CMB is receiving numerous change requests to the point where the amount of

requests would drop by modifying the baseline, then that is a good reason to change the

baseline. None of the other reasons should involve the baseline at all.

**15.** B. A UPS can provide line conditioning, adjusting power so that it is optimized for the

devices it serves and smoothing any power fluctuations; it does not offer any of the other

listed functions.

Chapter 10: Legal and Compliance Part 1 **323**

**16.** A. All deviations from the baseline should be documented, including details of the investigation

and outcome. We do not enforce or encourage deviations. Presumably, we would

already be aware of the deviation, so “revealing” is not a reasonable answer.

**17.** A. The more systems that be included in the baseline, the more cost-effective and scalable

the baseline is. The baseline does not deal with breaches or version control; those are the

provinces of the security office and CMB, respectively. Regulatory compliance might (and

usually will) go beyond the baseline and involve systems, processes, and personnel that are

not subject to the baseline.

**18.** C. Joint operating agreements can provide nearby relocation sites so that a disruption limited to

the organization’s own facility and campus can be addressed at a different facility and campus.

UPS and generators are not limited to serving needs for localized causes. Regulations do not

promote cost savings and are not often the immediate concern during BC/DR activities.

**19.** D. The Uptime Institute dictates 12 hours of generator fuel for all cloud datacenter tiers.

**20.** C. While hard drives may be useful in the kit (for instance, if they store BC/DR data such

as inventory lists, baselines, and patches), they are not necessarily required. All the other

items should be included.