Review Questions Chapter 6 Legal and Compliance

**1.** Which is the lowest level of the CSA STAR program?

**A.** Continuous monitoring

**B.** Self-assessment

**C.** Hybridization

**D.** Attestation

**2.** Which of the following is a valid risk management metric?

**A.** KPI

**B.** KRI

**C.** SLA

**D.** SOC

**3.** Which of the following frameworks focuses specifically on design implementation and

management?

**A.** ISO 31000:2009

**B.** HIPAA

**C.** ISO 27017

**D.** NIST 800-92

**4.** Which of the following frameworks identifies the top 8 security risks based on likelihood

and impact?

**A.** NIST 800-53

**B.** ISO 27000

**C.** ENISA

**D.** COBIT

**5.** The CSA STAR program consists of three levels. Which of the following is not one of those

levels?

**A.** Self-assessment

**B.** Third-party assessment-based certification

**C.** SOC 2 audit certification

**D.** Continuous monitoring–based certification

**6.** Which ISO standard refers to addressing security risks in a supply chain?

**A.** ISO 27001

**B.** ISO/IEC 28000:2007

**C.** ISO 18799

**D.** ISO 31000:2009

**7.** Which of the following is *not* a risk management framework?

**A.** NIST SP 800-37

**B.** European Union Agency for Network and Information Security (ENISA)

**C.** Key risk indicators (KRI)

**D.** ISO 31000:2009

**8.** Which of the following best define risk?

**A.** Threat coupled with a breach

**B.** Vulnerability coupled with an attack

**C.** Threat coupled with a threat actor

**D.** Threat coupled with a vulnerability

**9.** Which of the following is not a part of the ENISA Top 8 Security Risks of cloud

computing?

**A.** Vendor lock-in

**B.** Isolation failure

**C.** Insecure or incomplete data deletion

**D.** Availability

**10.** Which of the following is a risk management option that halts a business function?

**A.** Mitigation

**B.** Acceptance

**C.** Transference

**D.** Avoidance

**11.** Which of the following best describes a cloud carrier?

**A.** A person or entity responsible for making a cloud service available to consumers

**B.** The intermediary who provides connectivity and transport of cloud services between

cloud providers and cloud consumers

**C.** The person or entity responsible for keeping cloud services running for customers

**D.** The person or entity responsible for transporting data across the Internet

**12.** Which of the following methods of addressing risk is most associated with insurance?

**A.** Transference

**B.** Avoidance

**C.** Acceptance

**D.** Mitigation

**13.** Which of the following components are part of what a CCSP should review when looking at contracting with a cloud service provider?

**A.** The physical layout of the datacenter

**B.** Background checks for the provider’s personnel

**C.** Use of subcontractors

**D.** Redundant uplink grafts

**14.** A data custodian is responsible for which of the following?

**A.** The safe custody, transport, storage of the data, and implementation of business rules

**B.** Logging access and alerts

**C.** Data content

**D.** Data context

**15.** Which of the following is *not* a way to manage risk?

**A.** Enveloping

**B.** Mitigating

**C.** Accepting

**D.** Transferring

**16.** Which of the following is not a risk management framework?

**A.** Hex GBL

**B.** COBIT

**C.** NIST SP 800-37

**D.** ISO 31000:2009

**17.** Which of the following is not appropriate to include in an SLA?

**A.** The number of user accounts allowed during a specified period

**B.** Which personnel are responsible and authorized among both the provider and the customer

to declare an emergency and transition the service to contingency operation status

**C.** The amount of data allowed to be transmitted and received between the cloud provider

and customer

**D.** The time allowed to migrate from normal operations to contingency operations

**18.** What is the Cloud Security Alliance Cloud Controls Matrix (CCM)?

**A.** An inventory of cloud service security controls that are arranged into separate security

domains

**B.** An inventory of cloud services security controls that are arranged into a hierarchy of

security domains

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

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

**19.** Which of the following is not one of the types of controls?

**A.** Transitional

**B.** Administrative

**C.** Technical

**D.** Physical

**20.** Which of the following is not an example of an essential internal stakeholder?

**A.** IT analyst

**B.** IT director

**C.** CFO

**D.** HR director

Answers Chapter 6: Legal and Compliance

**1.** B. The lowest level is Level 1, which is self-assessment, Level 2 is an external third-party

attestation, and Level 3 is a continuous-monitoring program. Hybridization does not exist

as part of the CSA STAR program.

**2.** B. KRI stands for key risk indicator. KRIs are the red flags if you will in the world of risk

management. When these change, they indicate something is amiss and should be looked at

quickly to determine if the change is minor or indicative of something important.

**3.** A. ISO 31000:2009 specifically focuses on design implementation and management.

HIPAA refers to health care regulations, NIST 800-92 is about log management, and ISO

27017 is about cloud specific security controls.

**4.** C. ENISA specifically identifies the top 8 security risks based on likelihood and impact.

**5.** C. The SOC 2 report is not a part of the CSA Star program. It is a totally different audit

reporting standard developed by the AICPA.

**6.** B. ISO /IEC 28000-2007 applies to security controls in supply chains. The others are cloud

computing standards by have little to do with supply chain management.

**7.** C. Key risk indicators are useful, but they are not a framework. ISO 31000:2009 is an

international standard that focuses on designing, implementing, and reviewing risk management

processes and practices. NIST SP 800-37 is the Guide for Implementing the Risk

Management Framework (RMF), a methodology for handling all organizational risk in a

holistic, comprehensive, and continual manner. European Union Agency for Network and

Information Security (ENISA) identifies 35 types of risks organizations should consider but

goes further by identifying the top eight security risks based on likelihood and impact.

**8.** D. The best definition of risk is that of a threat coupled with a vulnerability.

**9.** D. The ENISA Top 8 Security Risks of Cloud Computing does not include availability,

even though it is certainly a risk that could be realized.

**10.** D. Avoidance halts the business process, mitigation entails using controls to reduce risk,

acceptance involves taking on the risk, and transference usually involves insurance.

**11.** B. A cloud carrier is the intermediary who provides connectivity and transport of cloud

services between cloud providers and cloud customers.

**12.** A. Avoidance halts the business process, mitigation entails using controls to reduce risk,

acceptance involves taking on the risk, and transference usually involves insurance.

**13.** C. The use of subcontractors can add risk to the supply chain and should be considered;

trusting the provider’s management of their vendors and suppliers (including subcontractors)

is important to trusting the provider. Conversely, the customer is not likely to be allowed to

review the physical design of the datacenter (or, indeed, even know the exact location of the

datacenter) or the personnel security specifics for the provider’s staff. “Redundant uplink

grafts” is a nonsense term used as a distractor.

**14.** A. A data custodian is responsible for the safe custody, transport, and storage of data, and

the implementation of business roles.

**15.** A. Enveloping is a nonsense term, unrelated to risk management. The rest are not.

**16.** A. Hex GBL is a reference to a computer part in Terry Pratchett’s fictional Discworld universe.

The rest are not.

**17.** B. Roles and responsibilities should be included in the contract, not the SLA; a good

method to determine whether something might belong in the SLA at all is figuring out

whether a numerical value is associated with it—in this case, the element involves names

and offices (roles), not numerical values, so it’s immediately recognizable as something that

isn’t appropriate for the SLA. Options A and C are explicitly defined by exact numbers and

are just the sort of aspects that belong in the SLA. Option D, the amount of time allowed to

transition between normal and contingency operations, is also an explicit numerical value,

but it is not a recurring event, regularly anticipated during each period of performance (or

shouldn’t be, anyway; if your cloud provider is fluctuating between normal and contingency

ops every performance period, you should probably find a new provider), so this is

something that can be defined once in the contract, and if the provider fails to perform in

the (hopefully rare) event it needs to be evaluated, then the provider is in breach, and there

should be remedies available other than the SLA. This is not an easy question, and understanding

the nuances can be difficult.

**18.** A. The CSA CCM is an inventory of cloud service security controls that are arranged into

separate security domains, not a hierarchy.

**19.** A. Transitional is not a term we associate with types of controls; the rest are.

**20.** A. An IT analyst is generally not high enough of a position to be able to provide quality

information to other stakeholders. However, the IT director would be in such a positon, as

would the others.