(ISC)^2 CCSP Certified Cloud Security Professional Official Study Guide

Second Edition

By Ben Malisow, CCSP, CISSP

Contents

FIGURE 1.1 Rapid scalability allows the customer to dictate the volume of resource usage.

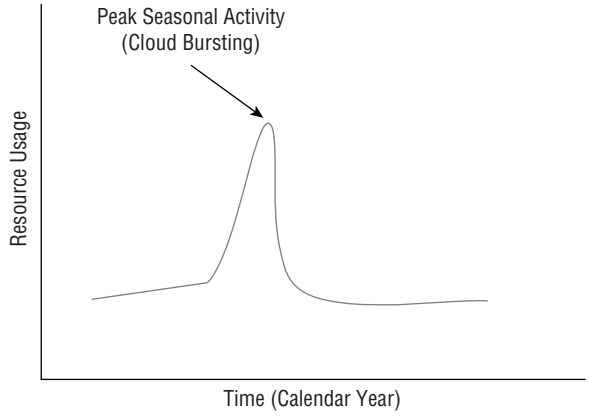


FIGURE 1.2 Cloud service models

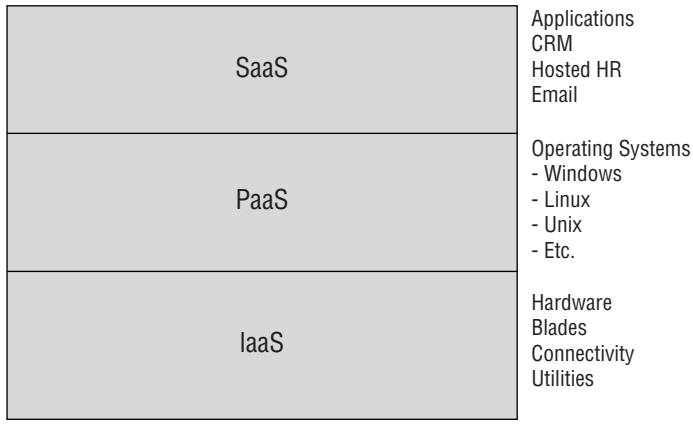


FIGURE 3.1 Data lifecycle

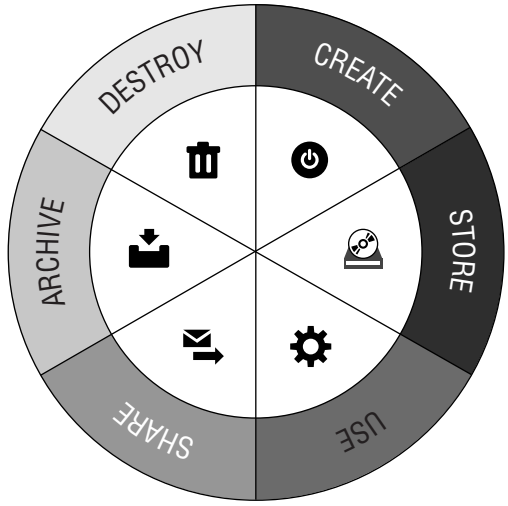


FIGURE 3.2 The copyright symbol

copyright
all rights reserved

FIGURE 4.1 Stages of the data lifecycle

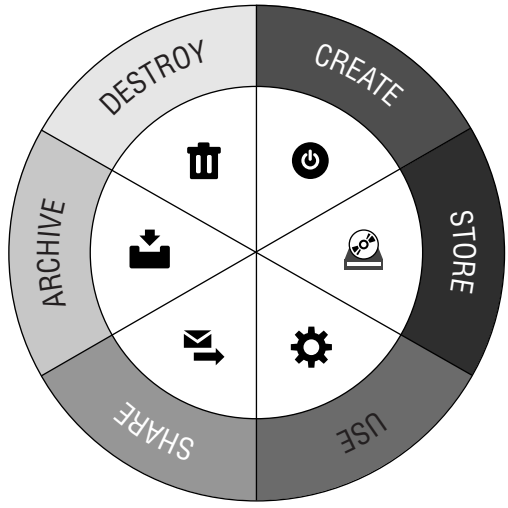


FIGURE 4.2 Basic tokenization architecture

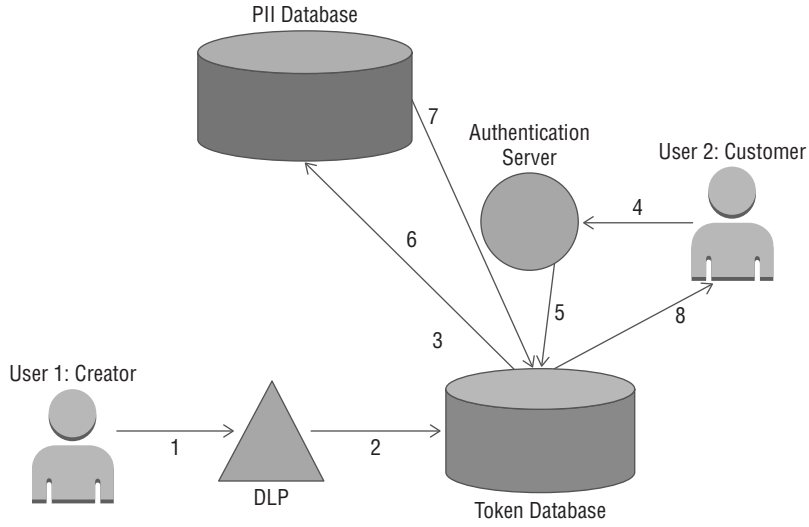


FIGURE 5.1 Responsibilities according to service model

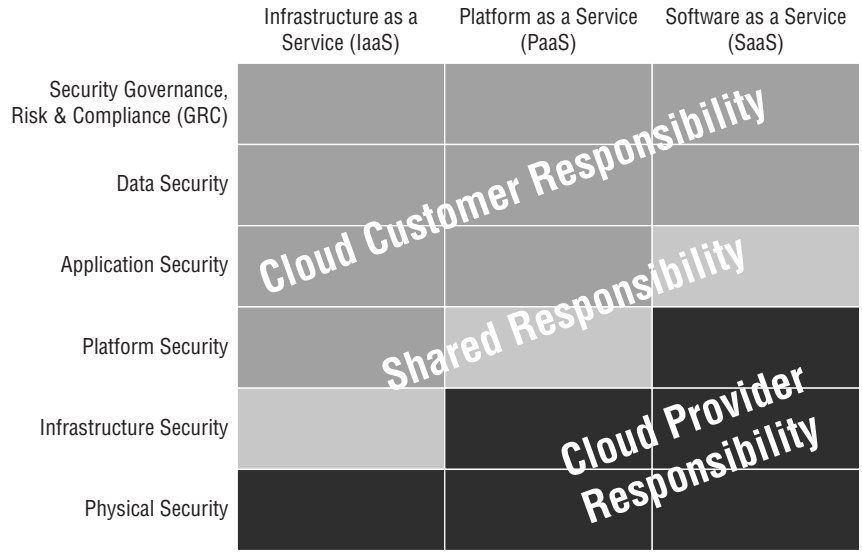


FIGURE 6.1 Responsibilities by service model

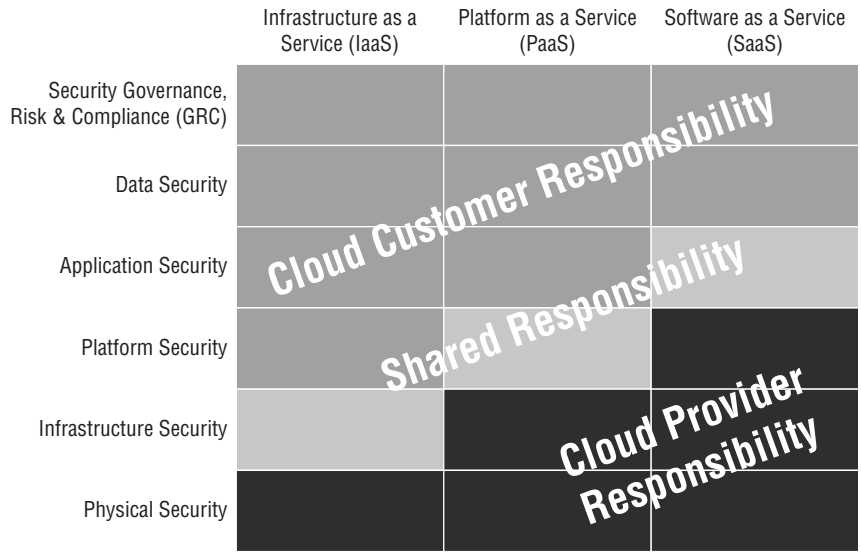


FIGURE 7.1 Customer/provider responsibilities, by service Model

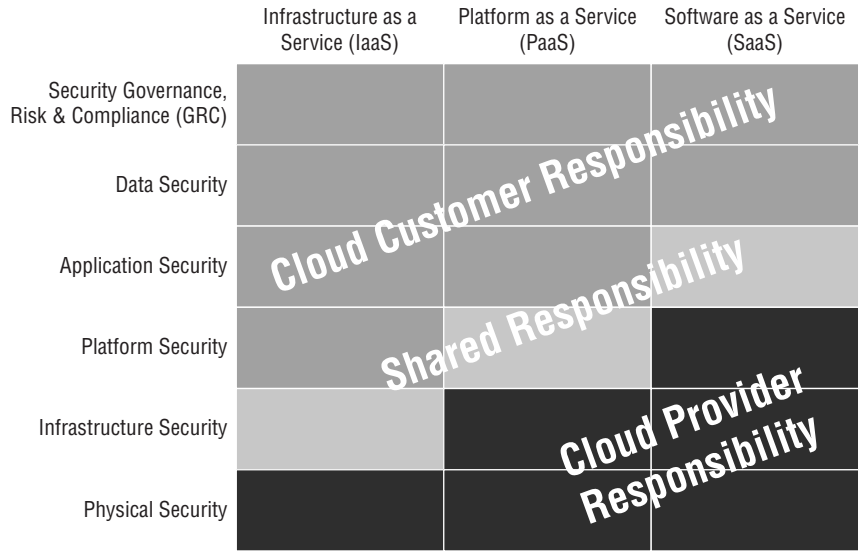


FIGURE 7.2 The cloud-secure software development lifecycle (SDLC)

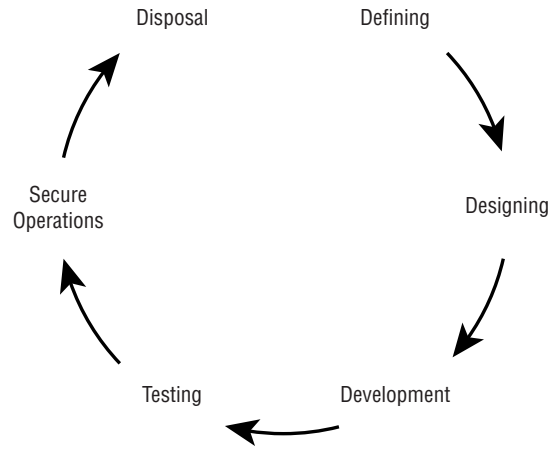
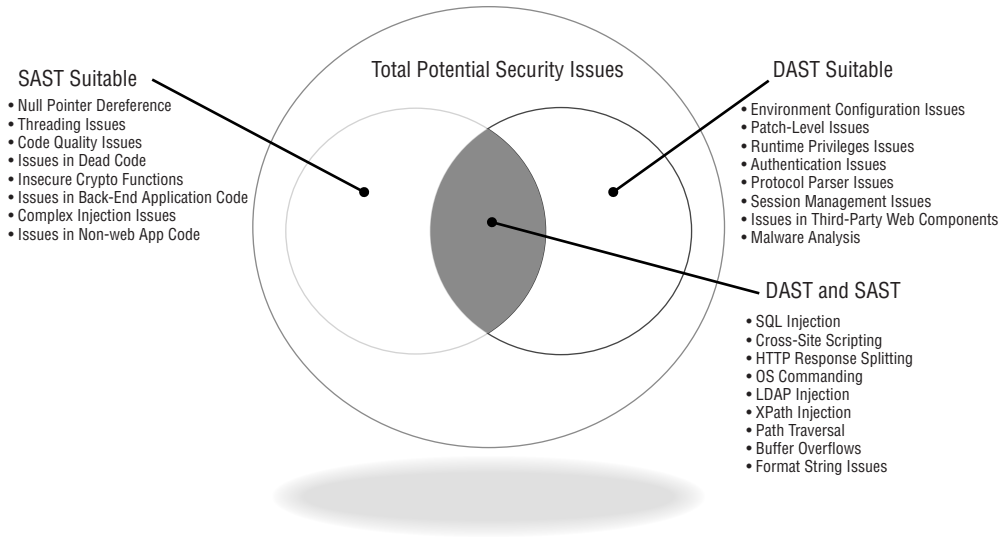


FIGURE 7.3 Testing Issues



Cloud Data Center Example

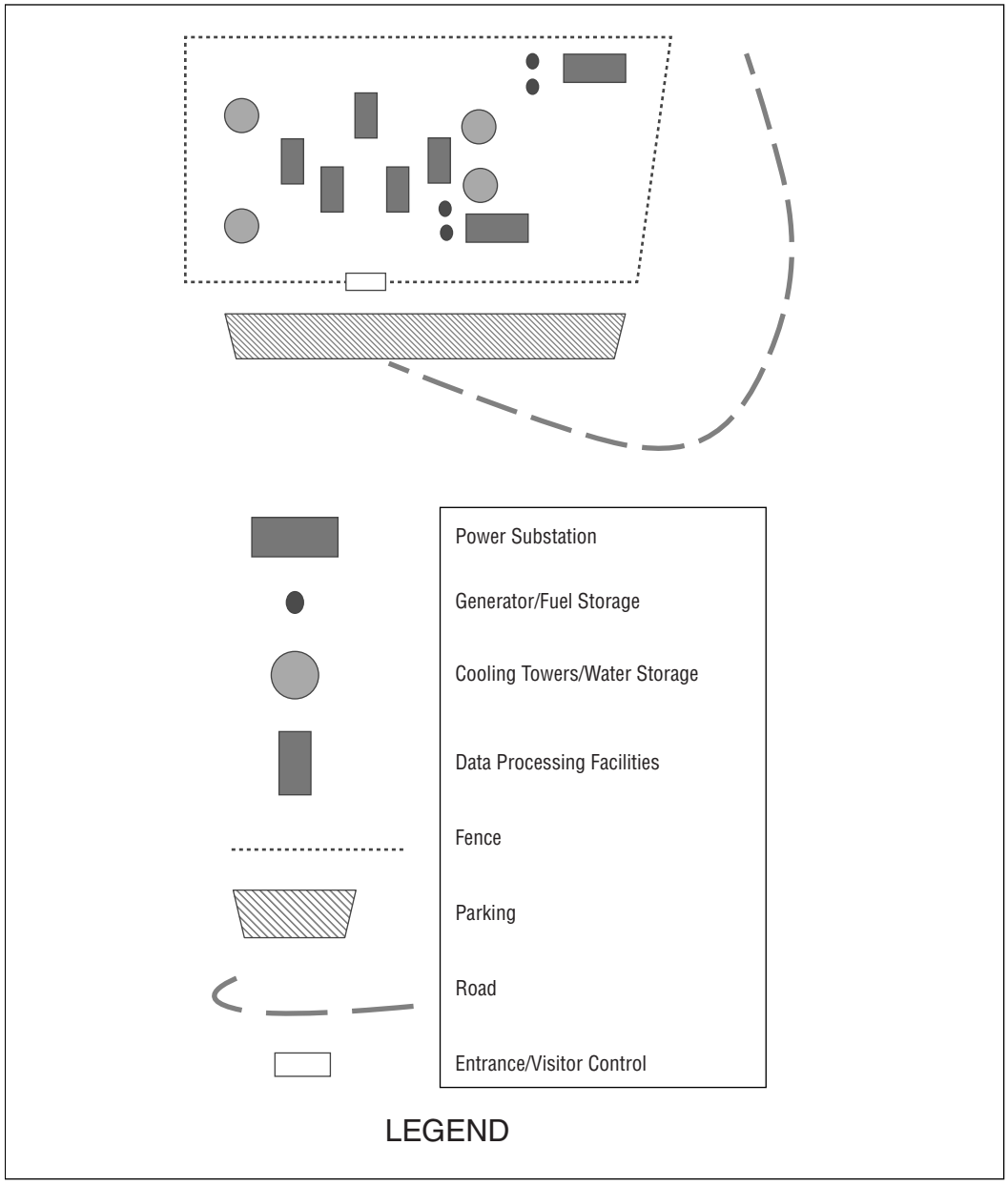


TABLE 10.1 Important US laws and regulations

Name	Purpose	Administrators	Enforcers
The Electronic Communication Privacy Act (ECPA)	Enhance laws restricting the government from putting wiretaps on phone calls, updating them to include electronic communication in the form of data.	*	*
Graham-Leach-Bliley Act (GLBA)	Allow banks to merge with and own insurance companies. Included in the law were stipulations that customer account information be kept secure and private and that customers be allowed to opt out of any information-sharing arrangements the bank or insurer might engage in.	FDIC, FFIEC	FDIC and DFI
Sarbanes–Oxley Act (SOX)	Increase transparency into publicly traded corporations' financial activities. Includes provisions for securing data and expressly names the traits of confidentiality, integrity, and availability.	SEC	SEC
Health Insurance Portability and Accountability Act (HIPAA)	Protect patient records and data, known as electronic protected health information (ePHI).	DHHS	OCR
Family Educational Rights and Privacy Act (FERPA)	Prevent academic institutions from sharing student data with anyone other than parents of students (up to age 18) or the students (after age 18).	Department of Education	Department of Education (Family Policy Compliance Office)
The Digital Millennium Copyright Act (DMCA)	Update copyright provisions to protect owned data in an Internet-enabled world. Makes cracking of access controls on copyrighted media a crime, and enables copyright holders to require any site on the Internet to remove content that may belong to the copyright holder.	**	**

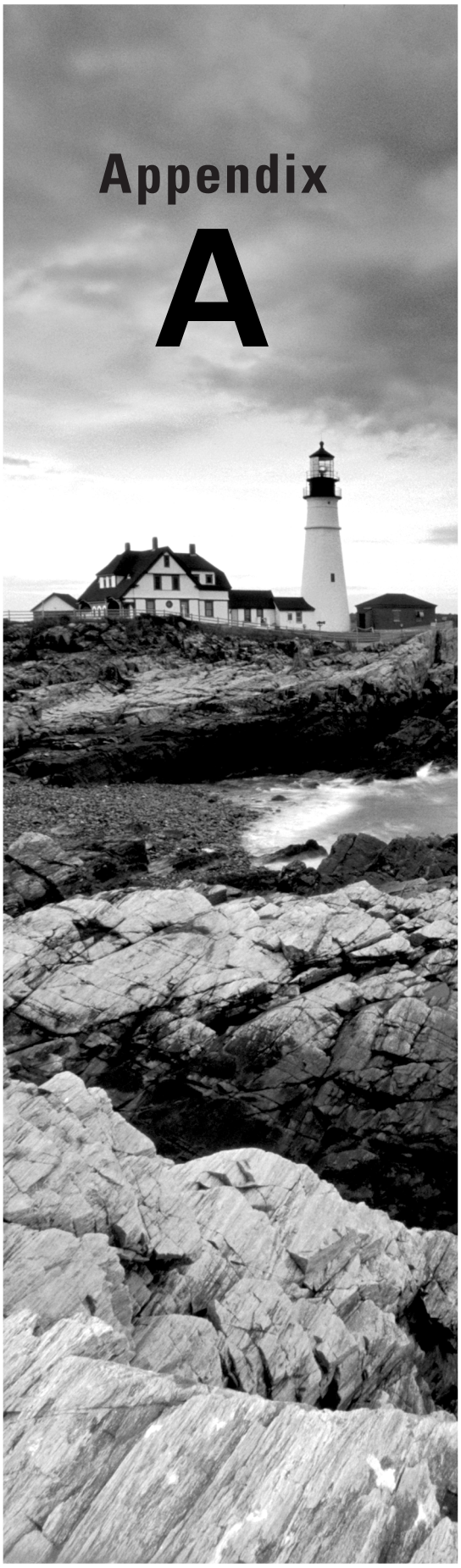
Name	Purpose	Administrators	Enforcers
Clarifying Lawful Overseas Use of Data (CLOUD Act)	Allows US law enforcement and courts to compel American companies to disclose data stored in foreign data centers; designed specifically for cloud computing situations (hence the name).	US federal courts	US federal law enforcement agencies

*The ECPA (and its subordinate parts, including the SCA) prevents the government from surveilling civilians. Ostensibly, the government would also be the entity enforcing and administering this law, and government law enforcement agencies would be the entities most likely to violate the law in the course of their activities. The reader can readily see the issues that might arise from this circular construct.

**The DMCA allows for aggrieved parties to bring civil suits to protect their interests, but it also has a provision that criminalizes a successful breach of access controls on copyrighted material.

TABLE 10.2 Countries and their laws relating to the EU Data Directive and Privacy Regulation

Nation	Federal PII law that complies with the EU Privacy Regulation	Notes
The EU	Yes	The EU comprises 27 member states (countries). The EU treats PII as a human right, with severely stringent protections for individuals.
United States	No	Personal privacy rights are often delineated in industry- and state-specific laws (such as GLBA for financial services and HIPAA for medicine), but there is no overarching federal law ensuring individual personal privacy.
Australia and New Zealand	Yes	Laws in these countries conform to the EU policies.
Argentina	Yes	Local law is specifically based on the EU guidance.
EFTA	Yes	A four-member body that includes Switzerland, Norway, Iceland, and Lichtenstein. Swiss law, in particular, provides stringent privacy protections, particularly for banking information.
Israel	Yes	
Japan	Yes	
Canada	Yes	The Personal Information Protection and Electronic Documents Act (PIPEDA) conforms to the EU Privacy Regulation.



Appendix

A

Answers to Written Labs

Chapter 1: Architectural Concepts

1. The Cloud Security Alliance website provides a lot of helpful information. Be sure to read the Guidance v4 document and review all of the helpful resources.
2. Answers will vary. Here are some possible responses:
   - The business might be concerned with unauthorized disclosure due to negligence or malice on the part of the cloud provider.
   - The business may be attracted to the dramatic cost savings offered by cloud computing.
   - The business may want to transition from a cumbersome legacy environment into something more flexible and modern.
3. The three cloud computing service models include IaaS, PaaS, and SaaS, and some of their common advantages and disadvantages include (but are not limited to) the following:
   - **IaaS:**

     Advantages: Reduced capital investment; increased redundancy for BC/DR; scalability

     Disadvantages: Reliance on cloud provider for security; responsibility for maintaining OS and apps retained
   - **PaaS:**

     Advantages: Multiple OS platforms to utilize, making it particularly good for testbed and software development purposes; all the advantages of IaaS

     Disadvantages: Reliance on cloud provider for updating OSs; responsibility for maintaining apps retained
   - **SaaS:**

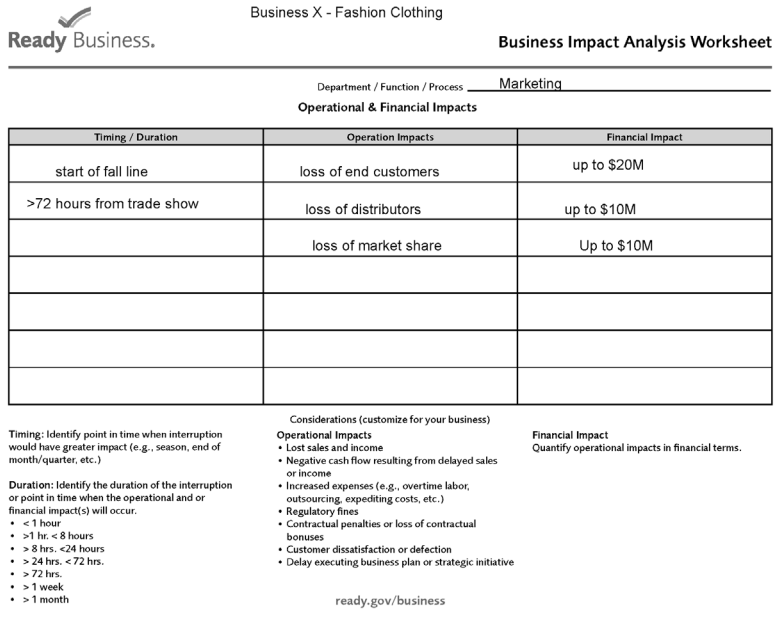
     Advantages: Cloud provider is responsible for all infrastructure, OSs, and apps; all the advantages of PaaS

     Disadvantages: Loss of all administrative control; may not have any insight into security

Chapter 2: Design Requirements

1. The Business Impact Analysis Worksheet is fairly straightforward and easy to use.
2. For this lab, I chose the marketing department, but any department or function can be analyzed.
3. For this lab, I chose the general loss of systems due to any and all possible reasons.
4. My worksheet, still in progress, looks like Figure A.1.

FIGURE A.1 Business impact analysis worksheet



Business X - Fashion Clothing

Ready Business.

Business Impact Analysis Worksheet

Department / Function / Process: Marketing

Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact
start of fall line	loss of end customers	up to $20M
>72 hours from trade show	loss of distributors	up to $10M
	loss of market share	Up to $10M

Considerations (customize for your business)

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.
- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Operational Impacts
- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

Financial Impact
Quantify operational impacts in financial terms.

ready.gov/business

Chapter 3: Data Classification

1. The NIST guidelines are helpful and easy to understand. Appendix D.1 provides a handy format that you can use for your devices.

2. Results should look like the example listed in 800-88, D.1:

   Example Statement of Cryptographic Erase Features:

   1. **Make/Model/Version/Media Type:** Acme hard drive model abc12345 version 1+. Media type is Legacy Magnetic media.
   2. **Key Generation:** A DRBG is used as specified in SP 800-90, with validation [number].
   3. **Media Encryption:** Media is encrypted with AES -256 media encryption in Cipher Block Chaining (CBC) mode as described in SP 800-38A. This device is FIPS 140 validated with certificate [number].
   4. **Key Level and Wrapping:** The media encryption key is sanitized directly during cryptographic erasure.

5. **Data Areas Addressed:** The device encrypts all data stored in the LBA-addressable space except for a preboot authentication and variable area and the device logs. Device log data is retained by the device following cryptographic erasure.
6. **Key Lifecycle Management:** As the MEK moves between wrapped, unwrapped, and rewrapped states, the previous instance is sanitized using three inverted overwrite passes.
7. **Key Sanitization Technique:** Three passes with a pattern that is inverted between passes.
8. **Key Escrow or Injection:** The device does not support escrow or injection of the keys at or below the level of the sanitization operation.
9. **Error Condition Handling:** If the storage device encounters a defect in a location where a key is stored, the device attempts to rewrite the location and the cryptographic erasure operation continues, reporting success to the user if the operation is otherwise successful.
10. **Interface Clarity:** The device has an ATA interface and supports the ATA Sanitize Device feature set `CRYPTO SCRAMBLE EXT` command and a TCG Opal interface with the ability to sanitize the device by cryptographically erasing the contents. Both of these commands apply the functionality described in this statement.

Chapter 4: Cloud Data Security

1. This white paper on preventing data leaks is just one of the many useful resources that ISACA provides. Be sure to explore others when you have the time.
2. An outstanding response would look something like this:

   According to the ISACA white paper on DLP solutions, the following operational risks might be involved in implementing DLP:

   Improperly Set DLP Tools. This is fairly obvious. The data owner must define the rules and categories associated with the organization's data or the DLP solution won't work in the manner intended. In fact, misconfigured DLP tools might actually harm the IT environment by adding extraneous overhead or responding to a significant amount of false positives.

   Improperly Sized Network DLP Module. If the DLP solution isn't correctly scoped for the organization's IT environment, it might miss a significant portion of network traffic, and data that should be prevented from leaving the organization's control might be allowed to go because the tool didn't even inspect it.

   Excessive Reporting and False Positives. See the first item; the rules and characteristics of suspect data have to be properly set by the data owner, and the tool has to understand the rules sufficiently to block only that data that fails instead of blocking legitimate traffic.

   Conflicts with the Traditional Environment. Interoperability will always be a concern for any new tool, including DLP.

Changes in Process of Infrastructure That Affect DLP Ability to Function Properly. The rules and identification capabilities for the DLP solution need to be updated as the environment changes; there is no "one-size-fits-all" DLP mechanism.

Improperly Placed DLP Modules. See the second point; the DLP tool might miss suspect traffic if it's placed in the wrong network location to monitor that traffic.

Undetected Failure of DLP Modules. Like any other toolset, if the DLP mechanisms aren't monitored and maintained properly and failure goes undetected, the organization will end up having a false sense of security.

Improperly Configured Directory Services. The DLP tools can only create an accurate audit chain when there is sufficient traceability in the environment to support that effort.

Chapter 5: Security in the Cloud

1. If possible, be sure to use the cloud providers' actual contracts when you do this. Discrepancies can exist between their marketing materials and contracts, and the contract is what is legally binding in the event of a later problem between you and the cloud provider.

2. Answers will vary. Be sure to record the URLs where you got the materials so you can refer back to them. Also, keep in mind that backup, pricing, and portability needs will vary from organization to organization. There is no one-size-fits-all solution.

Chapter 6: Responsibilities in the Cloud

1. The Cloud Security Alliance's STAR program is widely used. You should be sure to fully understand STAR.

2. This is the questionnaire that registered cloud providers fill out. It includes information on how they handle various aspects of security.

3. This is an important document. It tells you a lot about how a cloud provider provides its services. Take some time to really consider what the information in this document means, particularly in the context of your organization's needs.

4. The Registry lists various cloud providers who have each registered with the CSA.

5. If you have time, it would be a good idea to download several completed questionnaires for different providers and compare them too.

6. Answers will vary. An outstanding response will look like this:

   I chose to review the [name of specific product] from [name of specific provider]. The following three issues came to my attention:

   1. This provider is charging customers for malware and vulnerability scans. These should probably be functions included with the price of the service instead of additional costs.

2. The provider's response about collecting/creating metadata on its customers is vague and leaves room for doubt about what specific information it gathers on customer behavior. It says that the customer owns their virtual machines and that the provider doesn't access or collect the customer's data. Does the provider truly not have any idea how customers are using the service?
3. The provider is securing ecommerce transactions with SSL; it would be better if TLS was used instead.

Chapter 7: Cloud Application Security

1. Answers will vary. An outstanding response would look something like this:

   I use Microsoft's Office 365, an SaaS. The APIs include my browser (Mozilla's Firefox), and any plug-ins necessary to run the various 365 suite of applications; these can include some Java implementations, Microsoft's own specific plug-ins for Firefox (Microsoft Office 2010, Silverlight, and Windows Live Photo Manager), and any other multimedia APIs used for including material in Office work products (possibly including the plug-ins for Adobe Acrobat and the Widevine tools from Google). There may be other plug-ins and add-ons that Firefox uses to manipulate data while 365 is running.

2. The cloud software development lifecycle is extremely similar to other SDLCs. A couple of the major differences to note are the importance of inspecting secure remote access and strong authentication for development of apps that will be used in the cloud.

3. Answers will vary. The cloud application architecture includes many components. These include, but are not limited to, the following: APIs, tenant separation, cryptography, sandboxing, and application virtualization.

4. An identity management provider will be in charge of provisioning, maintaining, and deprovisioning identities on behalf of the cloud customer. This might include providing secure remote access, managing crypto keys, and federation of multiple resource providers.

Chapter 8: Operations Elements

1. Answers will vary. An example might look like this:

   The application I am using as a theoretical sample is a database of information regarding dogs. The primary key will be each dog's RFID chip number, and all other fields will describe characteristics of the dogs, such as weight, color, owner information (including contact data such as email and home address), and so forth. The organization (data owner) is a dog food and toy manufacturer, and it uses this database for targeted marketing

to groups of dog owners. The organization's staff (the user base) accesses the database through web portals.

2. STRIDE comprises Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. Using this model helps you quickly identify many possible points of failure.

3. Answers will vary. An example:

   The database might be subject to these three kinds of threats:

   - **Tampering with Data:** SQL injection. A malicious user (either internal or external) might try to enter SQL commands in data fields as a means to corrupt the data or affect the overall system.
   - **Controls:** Field validation should be included so that the program can detect SQL commands in data fields and not accept them.
   - **Information Disclosure:** Dog owner PII. Because the owners' PII is included in the database (home addresses), the organization should be careful to reduce the likelihood of the PII being disclosed to unauthorized parties, including the organization's employees who do not have a need to know that data.
   - **Controls:** Employ masking/obfuscation techniques so that unauthorized users do not see the PII content in those specific fields but instead see blank spaces or Xs.
   - **Denial of Service:** DDoS. Because access to the database is via the web, a DDoS attack against the servers could hinder user access to the data.
   - **Controls:** Deploy and utilize strong network security tools, such as properly configured routers, firewalls, and IDS/IPS systems, and ensure redundancy of all Internet connections (including DNS nodes).

Chapter 9: Operations Management

1. Answers will vary. Possible choices might include Kohler, Honda, Cummins, Subaru, and Hitachi.

2. Answers will vary. Be sure to compare the specifications for the generators you chose against the hypothetical loads you imagine for your data centers and against the ASHRAE standards.

3. Answers will vary. You should use the listed criteria (load, price, fuel) to justify your choice of preferred generator. The ASHRAE guidance is fairly detailed regarding specific ranges, based on the type, age, and location of the equipment. As you compare the generators, it is important to determine which guidance is most applicable to your facility and take into account any guidance and recommendations from the manufacturers regarding ambient ranges affecting performance parameters for their specific products.

Chapter 10: Legal and Compliance Part 1

1. Laws are dictated by legislatures and enforced by government. Regulations are created by governmental agencies and enforced by government. Standards are prescribed modes for certain types of activity; sources include industry bodies, certifying entities, or internal guidelines within organizations themselves. Contracts can also result in mandates, even if they are entered into voluntarily.

2. HIPAA now includes a number of rules that have been developed to address a range of issues. The two most often referred to are the Privacy Rule and the Security Rule. The Privacy Rule deals with the necessity to protect patient data (PHI), and the Security Rule deals with supporting the CIA triad in a medical organization.

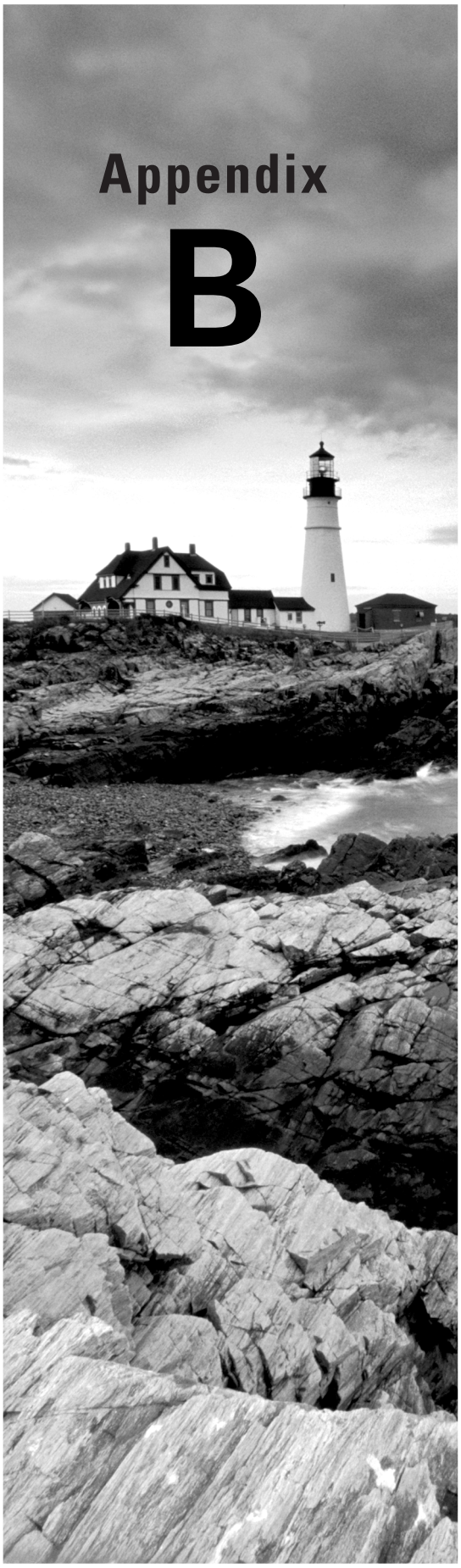
3. The SOC 1 report addresses only financial reporting activity and is of no interest to IT security practitioners. The SOC 2 describes IT security controls and comes in two types, Type 1 and Type 2. Type 1 covers the architecture and control framework design at a point in time, whereas Type 2 is a review of the actual controls as implemented over a period of time. The SOC 3 report is only an attestation that one of the SOC 2 reports has been performed, without any detail.

Chapter 11: Legal and Compliance Part 2

1. The CSA Star program and Open Certification Framework have been widely adopted. While many cloud providers meet their requirements, not all have, so it is still important to confirm this.

2. Answers will vary and might include NIST's 800-37 (Risk Management Framework), COSO, and COBIT.

3. Answers will vary and might include throughput, per-use prices, the customer's business drivers, BC/DR considerations, portability, and more.



Appendix

B

Answers to Review Questions

Chapter 1: Architectural Concepts

1. B. Programming as a service is not a common offering; the others are ubiquitous throughout the industry.

2. D. Virtualization allows scalable resource allocation; broadband connections allow users to have remote access from anywhere; encrypted connections allow for secure remote access. Smart hubs aren't widely used in cloud offerings.

3. A. Service-level agreements (SLAs) specify objective measures that define what the cloud provider will deliver to the customer.

4. C. Security is usually not a profit center and is therefore beholden to business drivers; the purpose of security is to support the business.

5. D. Lack of access is an availability issue.

6. B. CASBs don't usually offer BC/DR/COOP services; that's something offered by cloud providers.

7. D. The data on magnetic swipe cards isn't usually encrypted.

8. B. Risks, in general, can be reduced but never eliminated; cloud service, specifically, does not eliminate risk to the cloud customer because the customer retains a great deal of risk after migration.

9. B. Backups are still just as important as ever, regardless of where your primary data and backups are stored.

10. D. The gamer owns the console in their home. The gamer can turn it on and off at their discretion, sell it, or smash it with a hammer. The various members of a community cloud can all share the underlying resources of the community cloud as they choose. In this case, Sony, the game maker, the gamer, and the other players are all members of the community, and all share different underlying components as they choose.

11. B. This is the definition of vendor lock-out.

12. B. This is a nonsense term used as a red herring.

13. C. Under current laws in most jurisdictions, the data owner is responsible for any breaches that result in unauthorized disclosure of PII; this includes breaches caused by contracted parties and outsources services. The data owner is the cloud customer.

14. B. The business impact analysis is designed to ascertain the value of the organization's assets and learn the critical paths and processes.

15. A. Because ownership and usage is restricted to only the one organization, this is a private cloud.

16. B. This is the definition of a public cloud model.

17. D. This is the definition of a community cloud model.

18. B. PaaS allows the cloud customer to install any kind of software, including software to be tested, on an architecture that includes any desired OSs.

19. C. SaaS is the most comprehensive cloud offering, requiring little input and administration on the part of the cloud customer.

20. A. IaaS offers what is basically a hot/warm disaster recovery (DR) site, with hardware, connectivity and utilities, allowing the customer to build out any kind of software configuration (including choosing OSs).

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. However, this collection of information does not objectively tell us how useful an asset is.

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 $10 lock on the $5 bicycle) in addition to 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 is 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 applications, 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. A memorandum of agreement/understanding (MOA/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 by determining the criticality and value of assets.

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 challenging question, so don't be frustrated if you did not get it correct on the first try.

9. A. A firewall is a technological control. The safe and extinguisher are physical controls, and firing someone is an administrative control.

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. There is no such thing as "reclusion evaluation." Legislative mandates (laws) do not tell an organization which risks are acceptable except in very, very specific industries, and those are outliers. Contracts don't dictate acceptable risk for an organization; the organization should use its risk appetite to guide how it crafts contracts.

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

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. This question is good practice for the exam, where every word in each question and each answer is important.

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. Any particular, specific risk may be everlasting or transient, but it's not the case that all risks could be described by either of these terms.

Chapter 3: Data Classification

1. B. All the others are valid methods of data discovery; user-based is a red herring with no meaning.

2. C. All the others might be included in data labels, but we don't usually include data value since it is prone to change frequently and because it might not be information we want to disclose to anyone who does not have need to know.

3. B. All the others might be included in data labels, but we don't include delivery vendor, which is nonsense in this context.

4. D. All the others might be included in data labels, but multifactor authentication is a procedure used for access control, not a label.

5. D. All the others are data analytics methods, but *refractory iterations* is a nonsense term thrown in as a distractor.

6. B. The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer and is not in direct contact with the production data.

7. C. In legal terms, when *data processor* is defined, it refers to anyone who stores, handles, moves, or manipulates data on behalf of the data owner or controller. In the cloud computing realm, this is the cloud provider.

8. B. Hardware cannot be sanitized by deleting data. Deleting, as an operation, does not erase the data; it simply removes the logical pointers to the data for processing purposes. Burning, deletion, and drilling can all be used to sufficiently destroy the hardware to the point where data becomes irrecoverable.

9. D. All the elements except transference need to be addressed in each policy. Transference is not an element of policy.

10. B. We don't have physical ownership, control, or even access to the hardware devices holding the data, so physical destruction, including melting, is not an option. Overwriting is a possibility, but it is complicated by the difficulty of locating all the sectors and storage areas that might have contained our data and by the likelihood that constant backups in the cloud increase the chance we'll miss something as it's being overwritten. Crypto-shredding is the only reasonable alternative. Cold fusion is a distractor.

11. A. Copyrights are protected tangible expressions of creative works. The other options listed are answers to subsequent questions.

12. B. Patents protect processes (as well as inventions, new plant life, and decorative patterns). The other options listed are answers to other questions.

13. D. Confidential sales and marketing materials unique to the organization are trade secrets. The other options listed are answers to other questions.

14. D. Confidential recipes unique to the organization are trade secrets. The other options listed are answers to other questions.

15. C. Logos, symbols, phrases, and color schemes that describe brands are trademarks. The other options listed are answers to other questions.

16. C. The DMCA provision for takedown notices allows copyright holders to demand removal of suspect content from the web, and puts the burden of proof on whoever posted the material; this function has been abused by griefers, trolls, and overzealous content producers. There is no toll exemption in the DMCA. The decryption program prohibition makes DeCSS and other similar programs illegal. *Puppet plasticity* is a nonsense term used for a distractor.

17. B. The US Patent and Trademark Office accepts, reviews and approves applications for new patents. The USDA creates and enforces agriculture regulation. OSHA oversees workplace safety regulations. The SEC regulates publicly traded corporations.

18. C. IRM solutions use all these methods except for dip switch validity, which is a nonsense term.

19. D. The United States does not have a single, overarching personal privacy law; instead, the US often protects personal information by industry (HIPAA, GLBA, FERPA, and so forth). Belgium, like all EU member countries, adheres to the GDPR. Argentina's Personal Data Protection Act cleaves to the EU regulation, as does Japan's Act on the Protection of Personal Information.

20. B. IRM tools should include all the functions listed except for self-destruction, which might hurt someone.

Chapter 4: Cloud Data Security

1. B. *Data discovery* is a term used to describe the process of identifying information according to specific traits or categories. The rest are all methods for obscuring data.

2. D. SIEM is not intended to provide any enhancement of performance; in fact, a SIEM solution may decrease performance because of additional overhead. All the rest are goals of SIEM implementations.

3. B. DLP does not have anything to do with elasticity, which is the capability of the environment to scale up or down according to demand. All the rest are goals of DLP implementations.

4. B. DLP solutions may protect against inadvertent disclosure. Randomization is a technique for obscuring data, not a risk to data. DLP tools will not protect against risks from natural disasters or against impacts due to device failure.

5. A. DLP tools can identify outbound traffic that violates the organization's policies. DLP will not protect against losses due to performance issues or power failures. The DLP solution must be configured according to the organization's policies, so bad policies will attenuate the effectiveness of DLP tools, not the other way around.

6. C. AES is an encryption standard. Link encryption is a method for protecting communications traffic. Using one-time pads is an encryption method.

7. A. DLP tools need to be aware of which information to monitor and what information requires categorization (usually done upon data creation, by the data owners). DLPs can be implemented with or without physical access or presence. USB connectivity has nothing to do with DLP solutions.

8. B. In order to implement tokenization, there will need to be two databases: the database containing the raw, original data and the token database containing tokens that map to original data. Having two-factor authentication is nice, but certainly not required. Encryption keys are not necessary for tokenization. Two-person integrity does not have anything to do with tokenization.

9. D. Data masking does not support authentication in any way. All the others are excellent use cases for data masking.

10. A. DLP can be combined with IRM tools to protect intellectual property; both are designed to deal with data that falls into special categories. SIEMs are used for monitoring event logs, not live data movement. Kerberos is an authentication mechanism. Hypervisors are used for virtualization.

11. A. ITAR is a Department of State program. EAR is a Commerce Department program. Evaluation assurance levels are part of the Common Criteria standard from ISO. Information rights management tools are used for protecting electronic processing of intellectual property.

12. B. EAR is a Commerce Department program. ITAR is a State Department program. Evaluation assurance levels are part of the ISO's Common Criteria standard. Information rights management tools are used for protecting electronic processing of intellectual property.

13. B. Cryptographic keys should not be stored along with the data they secure, regardless of key length. We don't group crypto keys (doing so would violate the principle of secrecy necessary for keys to serve their purpose). Keys should be based on randomized (or pseudo-randomized) generation and not have any dependency.

14. D. We should do all of these except for requiring multifactor authentication. Multifactor authentication might be an element of access control for keys, but it is not specifically an element of key management.

15. A. The physical security of crypto keys is of some concern, but guards or vaults are not always necessary. Two-person integrity might be a good practice for protecting keys. The best answer to this question is option A, because it is always true, whereas the remaining options depend on circumstances.

16. D. All of these things should be considered when creating data archival policies except option D, which is a nonsense term.

17. B. The other options are the names of the phases, but they are out of proper order.

18. B. Cloud access security brokers provide IAM functions. Data loss, leak prevention, and protection are a family of tools used to reduce the possibility of unauthorized disclosure of sensitive information. SIEMs are tools used to collate and manage log data. AES is an encryption standard.

19. C. Databases store data in fields, in a relational motif. Object-based storage stores data as objects in a volume, with labels and metadata. File-based is a cloud storage architecture that manages the data in a hierarchy of files. A CDN stores data in caches of copied content near locations of high demand.

20. D. A CDN stores data in caches of copied content near locations of high demand. Object-based storage stores data as objects in a volume, with labels and metadata. File-based is a cloud storage architecture that manages the data in a hierarchy of files. Databases store data in fields, in a relational motif.

Chapter 5: Security in the Cloud

1. D. Elasticity is the name for the benefit of cloud computing where resources can be apportioned as necessary to meet customer demand. Obfuscation is a technique to hide full raw data sets, either from personnel who do not have need to know or for use in testing. Mobility is not a term pertinent to the CBK.

2. D. This is not a normal configuration and would not likely provide genuine benefit.

3. B. Background checks are controls for attenuating potential threats from internal actors; external threats aren't likely to submit to background checks.

4. B. IRM and DLP are used for increased authentication/access control and egress monitoring, respectively, and would actually decrease portability instead of enhancing it.

5. A. Dual control is not useful for remote access devices because we'd have to assign two people for every device, which would decrease efficiency and productivity. Muddling is a cocktail preparation technique that involves crushing ingredients. Safe harbor is a policy provision that allows for compliance through an alternate method rather than the primary instruction.

6. D. The cloud provider's resellers are a marketing and sales mechanism, not an operational dependency that could affect the security of a cloud customer.

7. A. State notification laws and the loss of proprietary data/intellectual property preexisted the cloud; only the lack of ability to transfer liability is new.

8. A. IaaS entails the cloud customer installing and maintaining the OS, programs, and data; PaaS has the customer installing programs and data; in SaaS, the customer only uploads data. In a community cloud, data and device owners are distributed.

9. C. NIST offers many informative guides and standards but nothing specific to any one organization. The cloud provider will not have prepared an analysis of lock-out/lock-in potential. Open-source providers can offer many useful materials but again, nothing specific to the organization.

10. B. Malware risks and threats are not affected by the terms of the cloud contract.

11. C. DoS/DDoS threats and risks are not unique to the multitenant architecture.

12. B. Hardened perimeter devices are more useful at attenuating the risk of external attack.

13. C. ISP redundancy is a means to control the risk of externalities, not internal threats.

14. D. Scalability is a feature of cloud computing, allowing users to dictate an increase or decrease in service as needed, not a means to counter internal threats.

15. C. Conflict of interest is a threat, not a control.

16. A. One-time pads are a cryptographic tool/method; this has nothing to do with BC/DR. All the other answers are benefits of using cloud computing for BC/DR.

17. C. Cryptographic sanitization is a means of reducing the risks from data remanence, not a way to minimize escalation of privilege.

18. B. Attackers prefer Type 2 hypervisors because the OS offers more attack surface and potential vulnerabilities. There are no Type 3 or 4 hypervisors.

19. B. Vendor lock-in is the result of a lack of portability, for any number of reasons. Masking is a means to hide raw datasets from users who do not have need to know. Closing is a nonsense term in this context.

20. C. Software developers often install backdoors as a means to avoid performing entire workflows when adjusting the programs they're working on; they often leave backdoors behind in production software, inadvertently or intentionally.

Chapter 6: Responsibilities in the Cloud

1. A. In IaaS, the cloud provider only owns the hardware and supplies the utilities. The customer is responsible for the OS, programs, and data. In PaaS and SaaS, the provider also owns the OS. There is no QaaS. That is a red herring.

2. D. While the provider might share any of the other options listed, the provider will not share administration of security controls with the customer.

3. B. The contract between the provider and customer enhances the customer's trust by holding the provider financially liable for negligence or inadequate service (although the customer remains legally liable for all inadvertent disclosures). Statutes, however, largely leave customers liable. The security control matrix is a tool for ensuring compliance with regulations. HIPAA is a statute.

4. D. The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting, and not relevant. The SOC 2 Type 2 is much more detailed and will most likely be held closely by the provider.

5. B. The SOC 3 is the least detailed, so the provider is not concerned about revealing it. The SOC 1 Types 1 and 2 are about financial reporting and not relevant. The SOC 2 Type 2 is much more detailed and will most likely be held closely by the provider.

6. D. The auditor should be impartial to the success of the target organization; consulting creates a conflict of interest.

7. B. Removing anti-malware agents. Hardening the operating system means making it more secure. Limiting administrator access, closing unused ports, and removing unnecessary services and libraries all have the potential to make an OS more secure. But removing anti-malware agents would actually make the system less secure. If anything, anti-malware agents should be added, not removed, as part of the hardening process.

8. C. Real-time environmental controls will not provide meaningful information and will not enhance trust. All the others will and do.

9. B. The customer does not administer on behalf of the provider. All the rest are possible options.

10. B. SOC 2 deals with the CIA triad. SOC 1 is for financial reporting. SOC 3 is only an attestation by the auditor. There is no SOC 4.

11. C. SOC 2 deals with the CIA triad. SOC 1 is for financial reporting. SOC 3 is only an attestation by the auditor. There is no SOC 4.

12. C. The provider may share audit and performance log data with the customer. The provider will most likely not share A and D since they reveal too much information about the provider's security program. B is already public information and does not enhance trust.

13. A. The customer always owns the data and will therefore always have access to it. The customer will never have administrative access to the provider's security controls, regardless of the model. The customer may or may not have administrative control over user permissions. The customer only has administrative power over the OS in an IaaS model.

14. D. Security is always contingent on business drivers and beholden to operational needs. The virtualization engine does not dictate security controls, and the hypervisor may vary (depending on its type and implementation). The SLAs do not drive security controls; they drive performance goals.

15. B. The customer currently always retains legal liability for data loss, even if the provider was negligent or malicious.

16. A. Knowledge of the physical layout and site controls could be of great use to an attacker, so they are kept extremely confidential. The other options are all red herrings.

17. B. Open-source software is available to the public, and often draws inspection from numerous, disparate reviewers. DBMS is not reviewed more or less than other software. All software in a production environment should be secure. That is not a valid discriminator for answering this question, so option C is not optimum. Proprietary software reviews are

limited to the personnel in the employ/under contract of the software developer, which narrows the perspective and necessarily reduces the amount of potential reviewers.

18. D. Firewalls do use rules, behavior analytics, and/or content filtering in order to determine which traffic is allowable. Firewalls ought not use random criteria, because any such limitations would be just as likely to damage protection efforts as enhance them.

19. C. A honeypot is meant to draw in attackers but not divulge anything of value. It should not use raw, production, or sensitive data.

20. C. Vulnerability assessments can only detect known vulnerabilities, using definitions. Some malware is known, as are programming flaws. Zero-day exploits, on the other hand, are necessarily unknown until discovered and exercised by an attacker and will therefore not be detected by vulnerability assessments.

Chapter 7: Cloud Application Security

1. B. The other answers all list aspects of SOAP.

2. B. The other answers are all possible stages used in software development.

3. D. The other answers all include aspects of the STRIDE model.

4. A. SAST involves source code review, often referred to as white-box testing.

5. B. This is the definition of authentication.

6. C. Options A and B are also correct, but C is more general and incorporates them both. D is incorrect because sandboxing does not take place in the production environment.

7. B. Options A and C are also correct, but included in B, making B the best choice. D is incorrect because we don't want unauthorized users gaining access.

8. A. In a trusted third-party model of federation, each member organization outsources the review and approval task to a third party they all trust. This makes the third party the identifier (it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).

9. B. Option A is incorrect because it refers to a specific application's security elements, meaning it is about an ANF, not the ONF. C is true, but not as complete as B, making B the better choice. D suggests that the framework contains only "some" of the components, which is why B (which describes "all" components) is better.

10. C. REST and SOAP are two common ways to build APIs. Although SOAP is based on XML, SOAP is more accurate. The other two answers are not used for making APIs.

11. B. Remember, there is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization). Therefore, the ANF is a subset of the ONF.

12. B. Option C is also true, but not as comprehensive as B. A and D are simply not true.

13. B. Option B is a description of the standard; the others are not.

14. D. This is the definition of threat modeling.

15. A. We don't use DAM in place of encryption or masking; DAM augments these options without replacing them. "Reactive or imperative" has no meaning in this context, and is only a distractor.

16. D. WAFs operate at Layer 7 of the OSI model.

17. D. Option D is the best, most general, and most accurate answer.

18. C. The other answers are true of SOAP.

19. C. DAST requires a runtime environment. All tests require money, so A is incorrect. Compartmentalization and inflation have no meaning in this context and are just distractors.

20. B. Physical sandboxing creates a test environment completely isolated from the production environment.

Chapter 8: Operations Elements

1. A. There are four tiers of the Uptime Institute's data center redundancy rating system, with 1 being the lowest and 4 the highest.

2. C. The other answers are distractors.

3. D. The development team should not be involved in direct testing of their own software because they bring personal biases and foreknowledge of the application and also because independent perspective is much more useful. All the other answers may be used as part of the testing team.

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 data centers that can be expected to be found in data centers 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 data center, 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. B. Tier 4 is the highest in the Uptime Institute standard; it is the only suitable tier for life-critical systems. Tier 2 does not provide sufficient redundancy/resiliency for supporting medical services. There are no Tiers 8 or X. As a test-taking tip, it helps to assume all the hospital's systems will migrate to the cloud unless otherwise stated. There could arguably be hospital systems that are not life-critical which wouldn't require Tier 4, but since that detail is not in the question, the broadest reading is appropriate.

15. D. The location of many data centers—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 data center.

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 because 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 because 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. C. Generators require fuel, and fuel is flammable. All the other answers do not represent an appreciable threat to human safety.

Chapter 9: Operations Management

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 data center 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 data center 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 data center to the next.

7. C. Generator power should be online before battery backups fail. The specific amount of time will vary between data centers.

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 data center 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 don't necessarily bear directly 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.

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 "revealed" is not a reasonable answer.

17. A. The more systems that are 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 systems 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 data center tiers.

20. C. The BC/DR kit is intended to be compact, and generator fuel is too cumbersome to include with the kit. All the other items should be included.

Chapter 10: Legal and Compliance Part 1

1. B. eDiscovery must collect and produce any data pertinent to the legal request that initiated the process.

2. A. Legal controls are those controls that are designed to comply with laws and regulations, whether they be local or international.

3. D. Plausibility, here, is a distractor and not specifically relevant to cloud forensics.

4. D. The value of data itself has nothing to do with it being considered a part of contractual PII even though the data may have value.

5. B. Mandatory breach reporting is the best example of regulated PII components. The rest are generally considered components of contractual PII.

6. B. Personal hobbies are not an element of privacy laws/contracts anywhere in the world (yet).

7. A. The primary advantage of external audits based on the choices given would be that of independence. External audits are typically more independent and therefore lead to more trustworthy results.

8. C. SOX was passed primarily to address the issues of audit independence, poor board oversight, and transparency of findings.

9. A. The SAS 70 was a report used in the past primarily for financial reporting and was oftentimes misused in the service provider context. The SSAE 18 standard and subsequent SOC reports are its successors.

10. A. The SOC 1 report focuses primarily on controls associated with financial services. While IT controls are certainly part of most accounting systems today, the focus is on the controls around those financial systems.

11. D. The SOC 3 report is more of an attestation than a full evaluation of controls associated with a service provider.

12. D. The AICPA is the organization responsible for generating and maintaining what are known as the Generally Accepted Accounting Principles in the United States.

13. A. GLBA deals with financial security and privacy. FERPA deals with data protection in the academic industry, HIPAA in the medical industry. SOX is a distractor here.

14. C. Wholesalers or distributors are generally not regulated, although the products they sell may be.

15. B. A SOC Type I report reviews a specific point in time as opposed to a report of effectiveness over a period of time.

16. D. A SOC Type II report reviews a period of time as opposed to a specific point in time.

17. C. The right to be forgotten is about the individual's right to have data removed from a provider at any time per their request. It is being tried in the EU at the moment but does not yet apply here in the United States.

18. D. Options A, B, and C are reasons leading up to the creation and passage of SOX.

19. C. The most important aspect of GLBA was the creation of a formal information security program.

20. D. Financial controls are not addressed by HIPAA.

Chapter 11: Legal and Compliance Part 2

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 help the organization identify and recognize changes to risk.

3. A. ISO 31000:2018 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 eight 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 specifically applies to security controls in supply chains. The others address other matters.

7. C. Key risk indicators are useful, but they are not a framework. ISO 31000:2018 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. The European Union Agency for Network and Information Security (ENISA) *Cloud Computing: Benefits, Risks, and Recommendations for Information Security* identifies the top eight cloud security risks.

8. D. There is no such thing as zero risk. All the other answers are distractors.

9. D. ENISA's top eight security risks of cloud computing do 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. Transference usually involves insurance. Avoidance halts the business process, acceptance involves taking on the risk, and mitigation entails using controls to reduce risk.

13. C. The use of subcontractors can add risk to the supply chain and should be considered; determining how much you can trust the provider's management of their vendors and suppliers (including subcontractors) is important. Conversely, the customer is not likely to be allowed to review the physical design of the data center (or, indeed, even know the exact location of the data center) or the personnel security specifics for the provider's staff. *Redundant uplink grafts* is a nonsense term used as a distractor.

14. C. Key risk indicators (KRIs) try to predict future risk, while key performance indicators (KPIs) examine events that have already happened. The other answers are just distractors.

15. A. *Enveloping* is a nonsense term, unrelated to risk management. The rest are valid ways to manage risk.

16. A. Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe. The rest are risk management frameworks.

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, C, D are explicitly defined by exact numbers that describe recurring events/circumstances and are just the sort of elements that belong in the SLA.

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 position, as would the others.