physical
sphere of influence so legitimate users feel a sense of ownership of that space.
C. These features are designed to make criminals think that those in the site are
more attentive, well resourced, and possibly alert.
D. These features are designed to make criminals feel uncomfortable by
providing many ways observers could potentially see them.



1183
118. Which of the following frameworks is a two-dimensional model that uses six basic communication interrogatives intersecting with different viewpoints to give
a holistic understanding of the enterprise?
A. SABSA
B. TOGAF
C. CMMI
D. Zachman

119. Not every data transmission incorporates the session layer. Which of the following
best describes the functionality of the session layer?
A. End-to-end data transmission
B. Application client/server communication mechanism in a distributed

environment
C. Application-to-computer physical communication
D. Provides application with the proper syntax for transmission
120. What is the purpose of the Logical Link Control (LLC) layer in the OSI model?
A. Provides a standard interface for the network layer protocol
B. Provides the framing functionality of the data link layer
C. Provides addressing of the packet during encapsulation
D. Provides the functionality of converting bits into electrical signals
121. Which of the following best describes why classless interdomain routing (CIDR)
was created?
A. To allow IPv6 traffic to tunnel through IPv4 networks
B. To allow IPSec to be integrated into IPv4 traffic
C. To allow an address class size to meet an organization’s need
D. To allow IPv6 to tunnel IPSec traffic
122. Johnetta is a security engineer at a company that develops highly confidential
products for various government agencies. Her company has VPNs set up to protect traffic that travels over the Internet and other nontrusted networks, but
she knows that internal traffic should also be protected. Which of the following is
the best type of approach Johnetta’s company should take?
A. Implement a data link technology that provides 802.1AE security functionality.
B. Implement a network-level technology that provides 802.1AE security functionality.

C. Implement TLS over L2TP.
D. Implement IPSec over L2TP.



1184
123. IEEE _____ provides a unique ID for a device. IEEE _____ provides data encryption, integrity, and origin authentication functionality. IEEE _____ carries out key agreement functions for the session keys used for data encryption. Each of these standards provides specific parameters to work within an IEEE _____ framework.
A. 802.1AF, 802.1AE, 802.1AR, 802.1X EAP-TLS
B. 802.1AT, 802.1AE, 802.1AM, 802.1X EAP-SSL
C. 802.1AR, 802.1AE, 802.1AF, 802.1X EAP-SSL
D. 802.1AR, 802.1AE, 802.1AF, 802.1X EAP-TLS

124. Under the principle of ethical disclosure, information systems security professionals must properly disclose _____ to the appropriate parties.
A. Vulnerabilities
B. Threats
C. Exploits
D. Incidents

125. Larry is a seasoned security professional and knows the potential dangers associated with using an ISP's DNS server for Internet connectivity. When Larry stays at a hotel or uses his laptop in any type of environment he does not fully trust, he updates values in his HOSTS file. Which of the following best describes why Larry carries out this type of task?
A. Reduces the risk of an attacker sending his system a corrupt ARP address that points his system to a malicious website
B. Ensures his host-based IDS is properly updated
C. Reduces the risk of an attacker sending his system an incorrect IP address-to-host mapping that points his system to a malicious website
D. Ensures his network-based IDS is properly synchronized with his host-based IDS
126. John has uncovered a rogue system on the company network that emulates a switch. The software on this system is being used by an attacker to modify frame tag values. Which of the following best describes the type of attack that has most likely been taking place?
A. DHCP snooping
B. VLAN hopping
C. Network traffic shaping
D. Network traffic hopping



1185

127. Frank is a new security manager for a large financial institution. He has been
told that the organization needs to reduce the total cost of ownership for many components of the network and infrastructure. The organization currently maintains many distributed networks, software packages, and applications. Which of the following best describes the cloud service models that Frank could leverage to obtain cloud services to replace on-premises network and infrastructure components
A. Infrastructure as a Service provides an environment similar to an operating

system, Platform as a Service provides operating systems and other major processing platforms, and Software as a Service provides specific applicationbased functionality.
B. Infrastructure as a Service provides an environment similar to a data center, Platform as a Service provides operating systems and other major processing platforms, and Software as a Service provides specific application-based functionality.
C. Infrastructure as a Service provides an environment similar to a data center, Platform as a Service provides application-based functionality, and Software as a Service provides specific operating system functionality.
D. Infrastructure as a Service provides an environment similar to a database, Platform as a Service provides operating systems and other major processing platforms, and Software as a Service provides specific application-based functionality.
128. Terry works in a training services provider where the network topology and access controls change very frequently. His boss tells him that he needs to implement a network infrastructure that enables changes to be made quickly and securely with minimal effort. What does Terry need to roll out?
A. Wi-Fi
B. Infrastructure as a Service
C. Software-defined networking
D. Software-defined wide area networking
129. On a Tuesday morning, Jami is summoned to the office of the security director,
where she finds six of her peers from other departments. The security director gives them instructions about an event that will be taking place in two weeks. Each of the individuals will be responsible for removing specific systems from the facility, bringing them to the offsite facility, and implementing them. Each individual will need to test the installed systems and ensure the configurations are
correct for production activities. What event is Jami about to take part in?
A. Parallel test
B. Full-interruption test
C. Simulation test
D. Structured walk-through test


130. While disaster recovery planning (DRP) and business continuity planning (BCP) are directed at the development of “plans,” _____ is the holistic management process that should cover both of them. It provides a framework for integrating resilience with the capability for effective responses that protects the

interests of the organization’s key stakeholders.
A. continuity of operations
B. business continuity management
C. risk management
D. enterprise management architecture

131. Your company enters into a contract with another company as part of which your company requires the other company to abide by specific security practices. Six months into the effort, you decide to verify that the other company is satisfying
these security requirements. Which of the following would you conduct?
A. Third-party audit
B. External (second-party) audit
C. Structured walk-through test
D. Full-interruption test

132. Which of the following statements is true about employee duress?
A. Its risks can be mitigated by installing panic buttons.
B. Its risks can be mitigated by installing panic rooms.
C. Its risks can be mitigated by enforcing forced vacations.
D. It can more easily be detected using the right clipping levels.

133. The main goal of the Wassenaar Arrangement is to prevent the buildup of military
capabilities that could threaten regional and international security and stability.
How does this relate to technology?
A. Cryptography is a dual-use tool.
B. Technology is used in weaponry systems.
C. Military actions directly relate to critical infrastructure systems.
D. Critical infrastructure systems can be at risk under this agreement.

134. Which world legal system is used in continental European countries, such as France and Spain, and is rule-based law, not precedent-based?
A. Civil (code) law system
B. Common law system
C. Customary law system
D. Mixed law system


135. Which of the following is not a correct characteristic of the Failure Modes and
Effect Analysis (FMEA) method?
A. Determining functions and identifying functional failures
B. Assessing the causes of failure and their failure effects through a structured

process
C. Structured process carried out by an identified team to address high-level security compromises
D. Identifying where something is most likely going to break and either fixing the flaws that could cause this issue or implementing controls to reduce the

impact of the break
136. A risk analysis can be carried out through qualitative or quantitative means.
It is important to choose the right approach to meet the organization’s goals. In a quantitative analysis, which of the following items would not be assigned a numeric value?
i. Asset value
ii. Threat frequency
iii. Severity of vulnerability
iv. Impact damage
v. Safeguard costs
vi. Safeguard effectiveness
vii. Probability
A. All of them
B. None of them
C. ii
D. vii
137. Uncovering restricted information by using permissible data is referred to as _____.
A. inference
B. data mining
C. perturbation
D. cell suppression


138. Meeta recently started working at an organization with no defined security processes. One of the areas she’d like to improve is software patching. Consistent
with the organizational culture, she is considering a decentralized or unmanaged model for patching. Which of the following is not one of the risks her organization would face with such a model?
A. This model typically requires users to have admin credentials, which violates

the principle of least privilege.
B. It will be easier to ensure that all software products are updated, since they
will be configured to do so automatically.
C. It may be difficult (or impossible) to attest to the status of every application in
the organization.
D. Having each application or service independently download the patches will lead to network congestion.
139. Clustering is an unsupervised machine learning approach that determines where
data samples naturally clump together. It does this by calculating the distance between a new data point and the existing clusters and assigning the point to the
closest cluster if, indeed, it is close to any of them. What is this approach typically
used for in cybersecurity?
A. Spam filtering
B. Anomaly detection

C. Network flow analysis
D. Signature matching
140. Sam wants to test the ability of her technical security controls to stop realistic attacks. Her organization is going through significant growth, which is also increasing the complexity of the networks and systems. To ensure she stays ahead of the adversaries, Sam wants to run these tests frequently. Which approach should she use?
A. Breach and attack simulations
B. Tabletop exercises
C. Red teaming
D. Synthetic transactions
Use the following scenario to answer Questions 141–142. Ron is in charge of updating his company's business continuity and disaster recovery plans and processes. After conducting a business impact analysis, his team has told him that if the company's e-commerce payment gateway was unable to process payments for 24 hours or more, this could drastically affect the survivability of the company. The analysis indicates that


after an outage, the payment gateway and payment processing should be restored within 13 hours. Ron's team needs to integrate solutions that provide redundancy, fault tolerance, and failover capability.
141. In the scenario, what does the 24-hour time period represent and what does the 13-hour time period represent, respectively?
A. Maximum tolerable downtime, recovery time objective
B. Recovery time objective, maximum tolerable downtime
C. Maximum tolerable downtime, recovery data period
D. Recovery time objective, data recovery period

142. Which of the following best describes the type of solution Ron's team needs to implement?
A. RAID and clustering
B. Storage area networks
C. High availability
D. Grid computing and clustering

Answers
1. D. While they are all issues to be concerned with, risk is a combination of probability and business impact. The largest business impact out of this list and in this situation is the fact that intellectual property for product development has been lost. If a competitor can produce the product and bring it to market quickly,

this can have a long-lasting financial impact on the company.
2. D. The attackers are the entities that have exploited a vulnerability; thus, they are
the threat agent.
3. C. In this situation the e-mail server most likely is misconfigured or has a programming flaw that can be exploited. Either of these would be considered a vulnerability. The threat is that someone would find out about this vulnerability
and exploit it. The exposure is allowing sensitive data to be accessed in an unauthorized manner.
4. C. Diameter is a protocol that has been developed to build upon the functionality
of RADIUS and TACACS+ while overcoming some of their limitations, particularly with regard to mobile clients. RADIUS uses UDP and cannot effectively deal well with remote access, IP mobility, and policy control. Mobile IP
is not an authentication and authorization protocol, but rather a technology that
allows users to move from one network to another and still use the same IP address.


5. C. DNS Security Extensions (DNSSEC, which is part of the many current implementations of DNS server software) works within a PKI and uses digital signatures, which allows DNS servers to validate the origin of a message to ensure
that it is not spoofed and potentially malicious. Suppose DNSSEC were enabled on server A, and a client sends it a DNS request for a resource that is not cached
locally. Server A would relay the request to one or more external DNS servers and, upon receiving a response, validate the digital signature on the message before accepting the information to make sure that it is from an authorized DNS server. So even if an attacker sent a message to a DNS server, the DNS server would discard it because the message would not contain a valid digital signature. DNSSEC allows DNS servers to send and receive only authenticated and authorized messages between themselves and thwarts the attacker’s goal of poisoning a DNS cache table.
6. C. The General Data Protection Regulation (GDPR) impacts every organization that holds or uses European personal data both inside and outside of Europe. In other words, if your company is a U.S.-based company that has never done business with the EU but it has an EU citizen working even as temporary staff (e.g., a summer intern), it probably has to comply with the GDPR or risk facing stiff penalties. There is no exclusion based on the nature of the relations between
the data subjects and the data controllers and processors.
7. B. A vulnerability is a lack or weakness of a control. The vulnerability is that the
user, who must be given access to the sensitive data, is not properly monitored to
deter and detect a willful breach of security. The threat is that any internal entity
might misuse given access. The risk is the business impact of losing sensitive

data.
One control that could be put into place is monitoring so that access activities can be closely watched.
8. C. A role-based access control (RBAC) model uses a centrally administrated set
of controls to determine how subjects and objects interact. An administrator does
not need to revoke and reassign permissions to individual users as they change jobs. Instead, the administrator assigns permissions and rights to a role, and users
are plugged into those roles.
9. A. Many (but not all) countries have data breach notification requirements, and these vary greatly in their specifics. While some countries have very strict requirements, others have laxer requirement, or lack them altogether. This requires the security professional to ensure compliance in the appropriate territory. Applying the most stringent rules universally (e.g., 24-hour notification)
is usually not a good idea from a business perspective. The term “best effort” is
not acceptable in countries with strict rules, nor is the notion that personally identifiable information (PII) is the only type of data that would trigger a mandatory notification.
10. D. Regression testing should take place after a change to a system takes place,
retesting to ensure functionality, performance, and protection.


11. B. ISO/IEC 27001 is a standard covering information security management systems (ISMSs), which is a much broader topic than supply chain risk management. The other three options are better answers because they are directly tied to this process: NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, directly addresses supply chain risk, and the insertion of hardware Trojans could happen at any point in the chain, upstream or downstream.
12. B. Various countries have data sovereignty laws that stipulate that anyone who
stores or processes certain types of data (typically personal data on their citizens),
whether or not they do so locally, must comply with those countries’ laws. Data localization laws, on the other hand, require certain types of data to be stored and
processed in that country (examples include laws in China and Russia).
13. B. Security through obscurity depends upon complexity or secrecy as a protection
method. Some organizations feel that since their proprietary code is not standards
based, outsiders will not know how to compromise its components. This is an insecure approach. Defense-in-depth is a better approach, with the assumption that anyone can figure out how something works.
14. C. ISO/IEC 27005 is the international standard for risk assessments and analysis.
15. C. ISO/IEC 27799 is a guideline for information security management in

health
organizations. It deals with how organizations that store and process sensitive medical information should protect it.
16. D. End-of-life (EOL) for an asset is that point in time when its manufacturer
is neither manufacturing nor sustaining it. In other words, you can't send it in for repairs, buy spare parts, or get technical assistance from the manufacturer. The related term, end-of-support (EOS), which is sometimes also called end-ofservice-life (EOSL), means that the manufacturer is no longer patching bugs or
vulnerabilities on the product.
17. B. A virtual private network (VPN) provides confidentiality for data being exchanged between two endpoints. While the use of VPNs may not be sufficient in every case, it is the only answer among those provided that addresses the question. The use of Secure Sockets Layer (SSL) is not considered secure. IEEE 802.1X is an authentication protocol that does not protect data in transit. Finally,
whole-disk encryption may be a good approach to protecting sensitive data, but only while it is at rest.
18. B. Threat modeling is the process of describing probable adverse effects on an organization's assets caused by specific threat sources. This modeling can use a variety of approaches, including attack trees and the MITRE ATT&CK framework. However, since the question refers to a report and neither of those approaches specifically points to a report, the more general answer of threat modeling is the best one.
19. B. A CAPTCHA is a skewed representation of characteristics a person must enter
to prove that the subject is a human and not an automated tool, as in a software robot. It is the graphical representation of data.


20. B. The CPO position was created mainly because of the increasing demands on organizations to protect a long laundry list of different types of data. This role
is responsible for ensuring that customer, organizational, and employee data is secure and kept secret, which keeps the organization out of criminal and civil courts and hopefully out of the headlines.
21. D. The correct sequence for the steps listed in the question is as follows:
i. Develop a risk management team.
ii. Identify company assets to be assessed.
iii. Calculate the value of each asset.
iv. Identify the vulnerabilities and threats that can affect the identified assets.

22. B. Synthetic transactions are scripted events that mimic the behaviors of real
users and allow security professionals to systematically test the performance of critical services. They are the best approach, because they can detect problems before users notice them. Real user monitoring (RUM) would rely on users encountering the problem, whereupon the system would automatically report it.
23. A. Data remanence refers to the persistence of data on storage media after it has

been deleted. Encrypting this data is the best of the listed choices because the recoverable data will be meaningless to an adversary without the decryption key. Retention policies are important, but are considered administrative controls that
don’t deal with remanence directly. Simply deleting the file will not normally render the data unrecoverable, nor will the use of SSDs even though these devices
will sometimes (though not always) make it difficult to recover the deleted data.
24. C. While all of these situations could have taken place, the most likely attack
type in this scenario is the use of a keylogger. Attackers commonly compromise personal computers by tricking the users into installing Trojan horses that have the capability to install keystroke loggers. The keystroke logger can capture
authentication data that the attacker can use to authenticate as a legitimate user
and carry out malicious activities.
25. B. IPSec is a suite of protocols used to provide VPNs that use strong encryption
and authentication functionality. It can work in two different modes: tunnel mode (payload and headers are protected) or transport mode (payload protection only). IPSec works at the network layer, not the data link layer.
26. C. In a typical public key infrastructure, the sender first needs to obtain the
receiver’s public key, which could be from the receiver or a public directory, and
then verify it. The sender needs to protect the symmetric session key as it is being
sent, so the sender encrypts it with the receiver’s public key. The receiver decrypts
the session key with the receiver’s private key.




27. C. Today, more organizations are implementing security information and event management (SIEM) systems. These products gather logs from various devices (servers, firewalls, routers, etc.) and attempt to correlate the log data and provide
analysis capabilities. Organizations also have different types of systems on a network (routers, firewalls, IDS, IPS, servers, gateways, proxies) collecting logs in
various proprietary formats, which requires centralization, standardization, and normalization. Log formats are different per product type and vendor.
28. D. Configuration management is a process aimed at ensuring that systems and controls are configured correctly and are responsive to the current threat and operational environments. Since the IPv6-to-IPv4 tunneling is not desirable, ensuring all devices are properly configured is the best approach of those listed.
Change management is a broader term that includes configuration management but is not the best answer listed because it is more general.
29. D. IoT devices run the gamut of cost, from the very cheap to the very expensive.

Cost, among the listed options, is the least likely to be a direct concern for a security professional. Lack of authentication, encryption, and update mechanisms are much more likely to be significant issues in any IoT adoption plan.
30. C. Each microservice lives in its own container and gets called as needed. If, for example, you see a spike in orders, you can automatically deploy a new container (in seconds), perhaps in a different host, and destroy it when you no longer need it. This contrasts with traditional servers that have fixed resources available and don't scale as well. Both approaches deal equally well with both web and database services and (properly deployed) have comparable security.
31. B. Extensible Access Control Markup Language (XACML), a declarative access control policy language implemented in XML and a processing model, describes how to interpret security policies. Service Provisioning Markup Language (SPML) is an XML-based language that allows for the exchange of provisioning data between applications, which could reside in one organization or many; allows for the automation of user management (account creation, amendments, revocation) and access entitlement configuration related to electronically published services across multiple provisioning systems; and allows for the integration and interoperation of service provisioning requests across various platforms. Security Assertion Markup Language (SAML) is an XML-based language that allows for the exchange of provisioning data between applications, which could reside in one organization or many.
32. C. A company must decide how to handle physical access control in the event of a power failure. In fail-safe mode, doorways are automatically unlocked. This is usually dictated by fire codes to ensure that people do not get stuck inside of a burning building. Fail-secure means that the door will default to lock.


33. C. Incident response typically requires humans in the loop. Next-generation firewalls (NGFWs) do not completely automate the process of responding to security incidents. NGFWs typically involve integrated IPS and signature sharing capabilities with cloud-based aggregators, but are also significantly more expensive than other firewall types.
34. D. Trolling is the term used to describe people who sow discord on various social platforms on the Internet by starting arguments or making inflammatory statements aimed at upsetting others. This is not a topic normally covered in security awareness training. Social engineering, phishing, and whaling are important topics to include in any security awareness program.
35. D. When clients digitally sign messages, this ensures nonrepudiation. Since the client should be the only person who has the client's private key, and only the client's public key can decrypt it, the e-mail must have been sent from the client. Digital signatures provide nonrepudiation protection, which is what this company needs.
36. D. Simple Authentication and Security Layer (SASL) is a protocol-independent authentication framework for authentication and data security in Internet protocols. It decouples authentication mechanisms from application protocols,

with the goal of allowing any authentication mechanism supported by SASL to be used in any application protocol that uses SASL. SASL's design is intended to allow new protocols to reuse existing mechanisms without requiring redesign of the mechanisms, and allows existing protocols to make use of new mechanisms without redesign of protocols.
37. D. Coupling is not considered a secure coding practice, though it does affect the
quality (and hence the security) of software. It is a measurement that indicates how much interaction one module requires to carry out its tasks. High (tight) coupling means a module depends upon many other modules to carry out its tasks. Low (loose) coupling means a module does not need to communicate with many other modules to carry out its job, which is better because the module is easier to understand and easier to reuse, and changes can take place to one module and not affect many modules around it.
38. A. A recovery time objective (RTO) is the amount of time it takes to recover from
a disaster, and a recovery point objective (RPO) is the amount of data, measured in time, that can be lost and be tolerable from that same event. The RPO is the acceptable amount of data loss measured in time. This value represents the earliest point in time by which data must be recovered. The higher the value of data, the more funds or other resources that can be put into place to ensure a smaller amount of data is lost in the event of a disaster. RTO is the maximum time period within which a business process must be restored to a designated service level after a disaster to avoid unacceptable consequences associated with
a break in business continuity.
39. B. Though laws vary around the world, many countries criminalize unauthorized
access, even if it lacked malicious intent.


40. A. XACML uses a Subject element (requesting entity), a Resource element (requested entity), and an Action element (types of access). XACML defines a declarative access control policy language implemented in XML.
41. B. The Mobile IP protocol allows location-independent routing of IP packets on
web-based environments. Each mobile device is identified by its home address. While away from its home network, a mobile node is associated with a care-of address, which identifies its current location, and its home address is associated
with the local endpoint of a tunnel to its home agent. Mobile IP specifies how a mobile device registers with its home agent and how the home agent routes packets to the mobile device.
42. D. A SIEM solution is a software platform that aggregates security information
and security events and presents them in a single, consistent, and cohesive manner.
43. D. The sensitivity of information is commensurate with the losses to an organization if that information were revealed to unauthorized individuals. Its criticality, on the other hand, is an indicator of how the loss of the information
would impact the fundamental business processes of the organization. While

replacement costs could factor into a determination of criticality, they almost never do when it comes to sensitivity.
44. C. Global organizations that move data across other country boundaries must be aware of and follow the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Since most countries have a different set of laws pertaining to the definition of private data and how it should be protected, international trade and business get more convoluted and can negatively affect the economy of nations. The OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so that data is properly protected and everyone follows the same type of rules.
45. B. Registered ports are 1024–49151, which can be registered with the Internet Assigned Numbers Authority (IANA) for a particular use. Vendors register specific ports to map to their proprietary software. Dynamic ports are 49152–65535 and are available to be used by any application on an "as needed" basis. Port numbers from 0 to 1023 are well-known ports.
46. A. The correct answer for cost/benefit analysis is the formula: (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization.
47. B. Each of the listed items are correct benefits or characteristics of cloud computing except "Cost of computing can be increased since it is a shared delivery model." The correct answer would be "Cost of computing can be decreased since it is a shared delivery model."



48. A. An architecture is a tool used to conceptually understand the structure and behavior of a complex entity through different views. An architecture provides different views of the system, based upon the needs of the stakeholders of that system.
49. B. Threat modeling is a systematic approach used to understand how different threats could be realized and how a successful compromise could take place. A threat model is a description of a set of security aspects that can help define a threat and a set of possible attacks to consider. It may be useful to define different threat models for one software product. Each model defines a narrow set of possible attacks to focus on. A threat model can help to assess the probability, the potential harm, and the priority of attacks, and thus help to minimize or eradicate the threats.
50. B. Many IDSs have "heuristic" capabilities, which means that the system gathers different "clues" from the network or system and calculates the probability an

attack is taking place. If the probability hits a set threshold, then the alarm sounds.
51. C. External auditors have certain advantages over in-house teams, but they will almost certainly not be as knowledgeable of internal processes and technology as the folks who deal with them on a daily basis.
52. C. In this example, staffers with lower security clearance than Don has could have deduced that the contract had been renewed by paying attention to the changes in their systems. The noninterference model addresses this specifically by dictating that no action or state in higher levels can impact or be visible to lower levels. In this example, the staff could learn something indirectly or infer something that they do not have a right to know yet.
53. B. HTML documents and e-mails allow users to attach or embed hyperlinks in any given text, such as the “Click Here” links you commonly see in e-mail messages or web pages. Attackers misuse hyperlinks to deceive unsuspecting users into clicking rogue links. The most common approach is known as URL hiding.
54. C. Personnel background checks are a common administrative (not technical) control. This type of audit would have nothing to do with the web applications themselves. The other three options (log reviews, code reviews, misuse case testing) are typical ways to verify the effectiveness of technical controls.
55. D. Statistical time-division multiplexing (STDM) transmits several types of data simultaneously across a single transmission line. STDM technologies analyze statistics related to the typical workload of each input device and make real-time decisions on how much time each device should be allocated for data transmission.
56. D. The actual voice stream is carried on media protocols such as RTP. RTP provides a standardized packet format for delivering audio and video over IP networks. RTP is a session layer protocol that carries data in media stream format, as in audio




and video, and is used extensively in VoIP, telephony, video conferencing, and other multimedia streaming technologies. It provides end-to-end delivery services and is commonly run over the transport layer protocol UDP. RTCP is used in conjunction with RTP and is also considered a session layer protocol. It provides out-of-band statistics and control information to provide feedback on QoS levels of individual streaming multimedia sessions.
57. A. Edge computing is a distributed system in which some computational and data storage assets are deployed close to where they are needed in order to reduce latency and network traffic. An edge computing architecture typically has three layers: end devices, edge devices, and cloud infrastructure.
58. C. A frequency analysis, also known as a statistical attack, identifies statistically

significant patterns in the ciphertext generated by a cryptosystem. For example, the number of zeroes may be significantly higher than the number of ones. This could show that the pseudorandom number generator (PRNG) in use may be biased.
59. D. IPSec is made up of two main protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides system authentication and integrity, but not confidentiality or availability. ESP provides system authentication, integrity, and confidentiality, but not availability. Nothing within IPSec can ensure the availability of the system it is residing on.
60. D. The ACID test concept should be incorporated into the software of a database.
ACID stands for:
• Atomicity Either the entire transaction succeeds or the database rolls it back to its previous state.
• Consistency A transaction strictly follows all applicable rules on all data affected.
• Isolation If transactions are allowed to happen in parallel (which most of them are), then they will be isolated from each other so that the effects of one don’t corrupt another. In other words, isolated transactions have the same effect whether they happen in parallel or one after the other.
• Durability Ensures that a completed transaction is permanently stored (for instance, in nonvolatile memory) so that it cannot be wiped by a power outage or other such failure.
61. B. In a Platform as a Service (PaaS) contract, the service provider normally takes care of all configuration, patches, and updates for the virtual platform. Jim would only have to worry about porting the applications and running them.
62. B. The biggest advantages of cloud computing are enhanced efficiency, performance, reliability, scalability, and security. Still, cloud computing is not a panacea. An organization must still carefully consider legal, contractual, and cost issues since they could potentially place the organization in a difficult position.


63. C. Shared responsibility addresses situations in which a cloud service provider is responsible for certain security controls, while the customer is responsible for others. It will be critical for Jim to delineate where these responsibilities lie. The other principles listed would presumably be equally important before and after the transition.
64. A. The aim of an attack surface analysis is to identify and reduce the amount of code accessible to untrusted users. The basic strategies of attack surface reduction are to reduce the amount of code running, reduce entry points available to

untrusted users, reduce privilege levels as much as possible, and eliminate unnecessary services. Attack surface analysis is generally carried out through specialized tools to enumerate different parts of a product and aggregate their findings into a numerical value. Attack surface analyzers scrutinize files, registry
keys, memory data, session information, processes, and services details.
65. B. The Capability Maturity Model Integration (CMMI) model outlines the necessary characteristics of an organization's security engineering process. It addresses the different phases of a secure software development life cycle, including
concept definition, requirements analysis, design, development, integration, installation, operations, and maintenance, and what should happen in each phase. It can be used to evaluate security engineering practices and identify ways
to improve them. It can also be used by customers in the evaluation process of a software vendor. Ideally, software vendors would use the model to help improve their processes, and customers would use the model to assess the vendor's practices.
66. D. VxLANs are designed to overcome two limitations of traditional VLANs: the limit of no more than 4,096 VLANs imposed by the 12-bit VLAN ID
(VID) field, and the need for VLANs to be connected to the same router port. Accordingly, VxLANs are mostly used by cloud service providers with hundreds of customers and by large organizations with a global presence.
67. D. These are all issues that are directly related to Kerberos. These items are as
follows:

- The Key Distribution Center (KDC) can be a single point of failure. If the KDC goes down, no one can access needed resources. Redundancy is necessary for the KDC.
- The KDC must be scalable to handle the number of requests it receives in a timely manner.
- Secret keys are temporarily stored on the users' workstations, which means it is
possible for an intruder to obtain these cryptographic keys.
- Session keys are decrypted and reside on the users' workstations, either in a cache or in a key table. Again, an intruder can capture these keys.
- Kerberos is vulnerable to password guessing. The KDC does not know if a dictionary attack is taking place.


68. A. Yes, the company should implement the control, as the value would be $25,000.
The cost/benefit calculation is (ALE before implementing safeguard) – (ALE after implementing safeguard) – (annual cost of safeguard) = value of safeguard to the organization, which in this case is $100,000 – $45,000 – $30,000 = $25,000.
69. D. The correct mappings for the individual standards are as follows:

- ISO/IEC 27002: Code of practice for information security controls
- ISO/IEC 27003: ISMS implementation guidance
- ISO/IEC 27004: ISMS monitoring, measurement, analysis, and evaluation
- ISO/IEC 27005: Information security risk management

• ISO/IEC 27007: ISMS auditing guidelines
70. B. Just-in-time (JIT) access temporarily elevates users to the necessary privileged access to perform a specific task, on a specific asset, for a short time. This approach mitigates the risk of privileged account abuse by reducing the time a threat actor has to gain access to a privileged account. While this could reduce some of the workload on the IT staff, it would have no impact on the time needed to reset a multitude of passwords.
71. C. End-to-end encryption happens within the applications. IPSec encryption takes place at the network layer. PPTP encryption takes place at the data link layer. Link encryption takes place at the data link and physical layers.
72. A. Hierarchical storage management (HSM) provides continuous online backup functionality. It combines hard disk technology with the cheaper and slower optical or tape jukeboxes. Storage area network (SAN) is made up of several storage systems that are connected together to form a single backup network.
73. C. The common law system is the only one that is based on previous interpretations of the law. This means that the system consists of both laws and court decisions in specific cases. Torts can be (and usually are) part of a common law system, but that would be an incomplete answer to this question.
74. B. It is important that evidence be relevant, complete, sufficient, and reliable to the case at hand. These four characteristics of evidence provide a foundation for a case and help ensure that the evidence is legally permissible.
75. B. Risk-based access control estimates the risk associated with a particular request in real time and, if it doesn’t exceed a given threshold, grants the subject access to the requested resource. This estimate can be based on multiple factors, including the risk history of similar requests. It is possible to improve a rule-based access control mechanism over time (based on historical data), but that would have to be a manual process and wouldn’t happen in real time.
76. C. SOAP enables programs running on different operating systems and written in different programming languages to communicate over web-based communication methods. SOAP is an XML-based protocol that encodes messages in a web service environment. SOAP actually defines an XML schema or a structure of how



communication is going to take place. The SOAP XML schema defines how objects communicate directly.
77. A. Each answer lists the correct definition mapping.
78. C. For an enterprise security architecture to be successful in its development and implementation, the following items must be understood and followed: strategic alignment, process enhancement, business enablement, and security effectiveness.
79. A. The OECD is an international organization where member countries come together to address economic, social, and governance challenges of a globalized

economy. Thus, the OECD came up with guidelines for the various countries to follow so data is properly protected and everyone follows the same type of rules.
80. A. The Zachman Framework is for business enterprise architectures, not security
enterprises. The proper definition mappings are as follows:
• Zachman Framework Model for the development of enterprise
architectures developed by John Zachman
• TOGAF Model and methodology for the development of enterprise
architectures developed by The Open Group
• DoDAF U.S. Department of Defense architecture framework that ensures
interoperability of systems to meet military mission goals
• SABSA Model and methodology for the development of information
security enterprise architectures
81. B. The ISO/IEC 27000 series provides a high-level overview of security program
requirements, while COBIT maps IT goals to enterprise goals to stakeholder needs through a series of transforms called cascading goals. COBIT specifies 13 enterprise and 13 alignment goals that take the guesswork out of ensuring we consider all dimensions in our decision-making processes.
82. D. This model was not built upon the SABSA model. All other characteristics are
true.
83. D. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) relies on the idea that the people working in a given environment best understand what is needed and what kind of risks they are facing. This places the
people who work inside the organization in the power positions of being able to make the decisions regarding what is the best approach for evaluating the security
of their organization.
84. B. An enterprise architecture framework is a conceptual model in which an architecture description is organized into multiple architecture views, where each view addresses specific concerns originating with the specific stakeholders.
Individual stakeholders have a variety of system concerns, which the architecture
must address. To express these concerns, each view applies the conventions of its
architecture viewpoint.

↟Appendix A: Comprehensive Questions


85. C. Fault tree analysis follows this general process. First, an undesired effect is
taken as the root, or top, event of a tree of logic. Then, each situation that has the
potential to cause that effect is added to the tree as a series of logic expressions.
Fault trees are then labeled with actual numbers pertaining to failure probabilities.
86. D. Security effectiveness deals with metrics, meeting service level agreement

(SLA) requirements, achieving return on investment (ROI), meeting set baselines, and providing management with a dashboard or balanced scorecard system. These are ways to determine how useful the current security solutions and architecture as a whole are performing.
87. D. Each answer provides the correct definition of the four levels that can be assigned to an organization during its evaluation against the CMMI model. This model can be used to determine how well the organization's processes compare to CMMI best practices and to identify areas where improvement can be made. Maturity Level 1 is Initial.
88. B. The ISRM policy should address all of the items listed except specific physical controls. Policies should not specify any type of controls, whether they are administrative, physical, or technical.
89. C. Each of these items should be considered before committing to an outsource partner or vendor.
90. D. The steps normally involved in the discovery of electronically stored information, or e-discovery, are identifying, preserving, collecting, processing, reviewing, analyzing, and producing the data in compliance with the court order. Data remanence is not part of e-discovery, though it could influence the process.
91. C. ISO/IEC 27004:2016, which is used to assess the effectiveness of an ISMS and the controls that make up the security program as outlined in ISO/IEC 27001. ISO/IEC 27004 provides guidance for ISMS monitoring, measurement, analysis, and evaluation.
92. B. Content distribution networks (CDNs) work by replicating content across geographically dispersed nodes. This means that regional users (those closest to a given node) will see improved responsiveness and could have tailored content delivered to them. It also means that mounting a successful DDoS attack is much more difficult. An ARP spoofing attack, however, takes place on the local area network and is therefore unrelated to the advantages of CDNs.
93. A. A CASB is a system that provides visibility and security controls for cloud services. A CASB monitors what users do in the cloud and applies whatever policies and controls are applicable to that activity.
94. C. A federated identity is a portable identity, and its associated entitlements, that can be used across business boundaries. It allows a user to be authenticated across multiple IT systems and enterprises. Single sign-on (SSO) allows users to enter credentials one time and be able to access all resources in primary and secondary network domains, but is not the best answer because it doesn't specifically address the capability to provide authentication across enterprises. A federated identity is a kind of SSO, but not every SSO implementation is federated.


95. B. HTML came from SGML, which came from GML. A markup language is a way to structure text and data sets, and it dictates how these will be viewed

and
used. When developing a web page, a markup language enables you to control how the text looks and some of the actual functionality the page provides.
96. A. XML is a universal and foundational standard that provides a structure for other independent markup languages to be built from and still allow for interoperability. Markup languages with various functionalities were built from XML, and while each language provides its own individual functionality, if they all follow the core rules of XML, then they are interoperable and can be used across different web-based applications and platforms.
97. B. A role-based access control (RBAC) model is based on the necessary operations
and tasks a user needs to carry out to fulfill her responsibilities within an organization.
This type of model lets access to resources be based on the user's roles. In hierarchical
RBAC, role hierarchies define an inheritance relation among roles.
98. C. Diameter is a more diverse centralized access control administration technique
than RADIUS and TACACS+ because it supports a wide range of protocols that often accompany wireless technologies. RADIUS supports PPP, SLIP, and traditional network connections. TACACS+ is a RADIUS-like protocol that is Cisco-proprietary. Kerberos is a single sign-on technology, not a centralized access
control administration protocol that supports all stated technologies.
99. A. An authoritative system of record (ASOR) is a hierarchical tree-like structure
system that tracks subjects and their authorization chains. The authoritative source is the "system of record," or the location where identity information originates and is maintained. It should have the most up-to-date and reliable identity information.
100. A. User provisioning refers to the creation, maintenance, and deactivation of
user objects and attributes as they exist in one or more systems, directories, or
applications, in response to business processes.
101. D. OpenID Connect (OIDC) is a simple authentication layer built on top of the OAuth 2.0 protocol. It allows transparent authentication and authorization of client resource requests. Though it is possible to use OAuth, which is an authorization standard, for authentication, you would do so by leveraging its OpenID Connect layer. Diameter and Kerberos are not well-suited for IDaaS.
102. A. The Service Provisioning Markup Language (SPML) allows for the exchange of provisioning data between applications, which could reside in one organization
or many. SPML allows for the automation of user management (account creation, amendments, revocation) and access entitlement configuration related to electronically published services across multiple provisioning systems. SPML also allows for the integration and interoperation of service provisioning requests
across various platforms.


103. B. In this scenario, Lynn is considered the principal, the airline company

is
considered the identity provider, and the hotel company that receives the user's authentication information from the airline company web server is considered the service provider. Security Assertion Markup Language (SAML) provides the authentication pieces to federated identity management systems to allow business-to-business (B2B) and business-to-consumer (B2C) transactions.
104. A. A service-oriented architecture (SOA) is way to provide independent services
residing on different systems in different business domains in one consistent manner. This architecture is a set of principles and methodologies for designing and developing software in the form of interoperable services.
105. B. The Bell-LaPadula model enforces the confidentiality aspects of access control
and consists of three main rules. The simple security rule states that a subject at a given security level cannot read data that resides at a higher security level.
The *-property rule (star property rule) states that a subject in a given security
level cannot write information to a lower security level. Finally, the strong star
property rule states that a subject who has read and write capabilities can only perform both of those functions at the same security level; nothing higher and nothing lower.
106. D. In the system design phase, the software development team gathers system requirement specifications and determines how the system will accomplish design goals, such as required functionality, compatibility, fault tolerance, extensibility,
security, usability, and maintainability. The attack surface analysis, together with the threat model, inform the developers' decisions because they can look at proposed architectures and competing designs from the perspective of an attacker.
This allows them to develop a more defensible system. Though it is possible to start the threat model during the earlier phase of requirements gathering, this modeling effort is normally not done that early. Furthermore, the attack surface cannot be properly studied until there is a proposed architecture to analyze. Performing this activity later in the SDLC is less effective and usually results in
security being "bolted on" instead of "baked in."
107. B. OAuth is an open standard for authorization to third parties. It lets you
authorize a web application to use something that you control at a different website. For instance, if users wanted to share an article in the web app directly to
their LinkedIn account, the system would ask them for access to their accounts in
LinkedIn. If they agree, they'd see a pop-up from LinkedIn asking whether they want to authorize the web app to share a post. If they agree to this, the web app
gains access to all their contacts until they rescind this authorization.
108. A. Each CPU type has a specific architecture and set of instructions that it
can carry out. The application must be developed to work within this CPU architecture and compiled into machine code that can run on it. This is why one application may work on an Intel processor but not on an AMD processor. There

are portable applications that can work on multiple architectures and operating systems, but these rely on a runtime environment.



109. C. According to Veracode, seven in ten applications use at least one open-source software library with a security flaw, which makes those applications vulnerable. This estimate doesn't include proprietary libraries, which are probably even more insecure because they haven't been subjected to the same amount of scrutiny as open-source ones. This is the main risk in using software libraries.

110. A. Dynamic application security testing (DAST), which is also known as dynamic analysis, refers to the evaluation of a program in real time, while it is running. It is the only one of the answers that is effective for analyzing software without having access to the actual source code.

111. C. Attackers have identified programming errors in operating systems that allow them to "starve" the system of its own memory. This means the attackers exploit a software vulnerability that ensures that processes do not properly release their memory resources. Memory is continually committed and not released, and the system is depleted of this resource until it can no longer function. This is an example of a denial-of-service attack.

112. A. Attribute-based access control (ABAC) is based on attributes of any component of the system. It is the most granular of the access control models.

113. A. The primary reason to use Kerberos is that the principals do not trust each other enough to communicate directly; they only trust the Key Distribution Center (KDC). This is a strength, not a weakness, of the system, but it does point to the fact that if only the KDC can vouch for identities, this creates a single point of failure. The fact that secret keys are stored on users' workstations, albeit temporarily, presents an attack opportunity for threat actors, who can also perform password attacks on the system.

114. A. The depth of field refers to the portion of the environment that is in focus when shown on the monitor. The depth of field varies, depending upon the size of the lens opening, the distance of the object being focused on, and the focal length of the lens. The depth of field increases as the size of the lens opening decreases, the subject distance increases, or the focal length of the lens decreases. So if you want to cover a large area and not focus on specific items, it is best to use a wide-angle lens and a small lens opening.

115. B. In a preaction system, a link must melt before the water will pass through the sprinkler heads, which creates the delay in water release. This type of

suppression
system is best in data-processing environments because it allows time to deactivate
the system if there is a false alarm.
116. B. A preaction system has a link that must melt before water is released. This is
the mechanism that provides the delay in water release. A deluge system has wide open sprinkler heads that allow a lot of water to be released quickly. It does not
have a delaying component.



1205
117. D. CPTED encourages natural surveillance, the goal of which is to make criminals
feel uncomfortable by providing many ways observers could potentially see them and to make all other people feel safe and comfortable by providing an open and well-designed environment. The other answers refer to the other three CPTED strategies, which are natural access control, territorial reinforcement, and
maintenance, respectively.
118. D. The Zachman Framework is a two-dimensional model that uses six basic communication interrogatives (What, How, Where, Who, When, and Why) intersecting with different viewpoints (Executives, Business Managers, System Architects, Engineers, Technicians, and Enterprise-wide) to give a holistic understanding of the enterprise. This framework was developed in the 1980s and is based on the principles of classical business architecture that contain rules that
govern an ordered set of relationships.
119. B. The communication between two pieces of the same software product that reside on different computers needs to be controlled, which is why session layer protocols even exist. Session layer protocols take on the functionality of middleware, enabling software on two different computers to communicate.
120. A. The data link layer has two sublayers: the Logical Link Control (LLC) and
Media Access Control (MAC) layers. The LLC sublayer provides a standard interface for whatever network protocol is being used. This provides an abstraction layer so that the network protocol does not need to be programmed to communicate with all of the possible MAC-level protocols (Ethernet, WLAN, frame relay, etc.).
121. C. A Class B address range is usually too large for most companies, and a Class C
address range is too small, so CIDR provides the flexibility to increase or decrease
the class sizes as necessary. CIDR is the method to specify more flexible IP address
classes.
122. A. 802.1AE is the IEEE MAC Security (MACSec) standard, which defines a security infrastructure to provide data confidentiality, data integrity, and data
origin authentication. Where a VPN connection provides protection at the higher networking layers, MACSec provides hop-by-hop protection at layer 2.
123. D. 802.1AR provides a unique ID for a device. 802.1AE provides data

encryption,
integrity, and origin authentication functionality. 802.1AF carries out key agreement
functions for the session keys used for data encryption. Each of these standards provides specific parameters to work within an 802.1X EAP-TLS framework.
124. A. As information systems security professionals, if we discover a vulnerability, we
have an ethical obligation to properly disclose it to the appropriate parties. If the
vulnerability is in our own product, we need to notify our customers and partners
as soon as possible. If it is in someone else's product, we need to notify the vendor
or manufacturer immediately so they can fix it. The goal of ethical disclosure is
to inform anyone who might be affected as soon as feasible, so a patch can be developed before any threat actors become aware of the vulnerability.


125. C. The HOSTS file resides on the local computer and can contain static hostname-to-IP mapping information. If you do not want your system to query a DNS server, you can add the necessary data in the HOSTS file, and your system will first check its contents before reaching out to a DNS server. Some people use these files to reduce the risk of an attacker sending their system a bogus IP address that points them to a malicious website.
126. B. VLAN hopping attacks allow attackers to gain access to traffic in various
VLAN segments. An attacker can have a system act as though it is a switch. The system understands the tagging values being used in the network and the trunking protocols, and can insert itself between other VLAN devices and gain access to the traffic going back and forth. Attackers can also insert tagging values
to manipulate the control of traffic at the data link layer.
127. B. The most common cloud service models are

• Infrastructure as a Service (IaaS) Cloud service providers offer the infrastructure environment of a traditional data center in an on-demand delivery method.
• Platform as a Service (PaaS) Cloud service providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment.
• Software as a Service (SaaS) Cloud service providers give users access to specific application software (e.g., CRM, e-mail, and games).
128. C. Software-defined networking (SDN) is an approach to networking that relies
on distributed software to provide unprecedented agility and efficiency. Using SDN, it becomes much easier to dynamically route traffic to and from newly provisioned services and platforms. It also means that a service or platform can be quickly moved from one location to another and the SDN will just as quickly update traffic-flow rules in response to this change.
129. A. Parallel tests are similar to simulation tests, except that parallel tests include

moving some of the systems to the offsite facility. Simulation tests stop just short
of the move. Parallel tests are effective because they ensure that specific systems
work at the new location, but the test itself does not interfere with business operations at the main facility.
130. B. While DRP and BCP are directed at the development of plans, business continuity management (BCM) is the holistic management process that should cover both of them. BCM provides a framework for integrating resilience with the capability for effective responses in a manner that protects the interests of
the organization's key stakeholders. The main objective of BCM is to allow the organization to continue to perform business operations under various conditions.
BCM is the overarching approach to managing all aspects of BCP and DRP.

↟Appendix A: Comprehensive Questions

1207
131. B. An external audit (sometimes called a second-party audit) is one conducted by
(or on behalf of ) a business partner to verify contractual obligations. Though this
audit could be conducted by a third party (e.g., an auditing firm hired by either
party), it is still considered an external audit because it is being done to satisfy an
external entity.
132. A. Duress is the use of threats or violence against someone in order to force them
to do something they don't want to do. A popular example of a countermeasure for duress is the use of panic buttons by bank tellers. A panic room could conceivably be another solution, but it would only work if employees are able to get in and lock the door before an assailant can stop them, which makes it a generally poor approach.
133. A. The Wassenaar Arrangement implements export controls for "Conventional Arms and Dual-Use Goods and Technologies." The main goal of this arrangement is to prevent the buildup of military capabilities that could threaten regional and
international security and stability. So, everyone is keeping an eye on each other
to make sure no one country's weapons can take everyone else out. One item the agreement deals with is cryptography, which is considered a dual-use good because it can be used for both military and civilian purposes. The agreement recognizes the danger of exporting products with cryptographic functionality to countries that are in the "offensive" column, meaning that they are thought to
have friendly ties with terrorist organizations and/or want to take over the world
through the use of weapons of mass destruction.
134. A. The civil (code) law system is used in continental European countries such as
France and Spain. It is a different legal system from the common law system used in the United Kingdom and United States. A civil law system is rule-based law,

not precedent-based. For the most part, a civil law system is focused on codified law—or written laws.

135. C. FMEA is a method for determining functions, identifying functional failures, and assessing the causes of failure and their failure effects through a structured process. It is commonly used in product development and operational environments. The goal is to identify where something is most likely going to break and either fix the flaws that could cause this issue or implement controls to reduce the impact of the break.

136. B. Each of these items would be assigned a numeric value in a quantitative risk analysis. Each element is quantified and entered into equations to determine total and residual risks. Quantitative risk analysis is more of a scientific or mathematical approach to risk analysis compared to qualitative.

137. A. Aggregation and inference go hand in hand. For example, a user who uses data from a public database to figure out classified information is exercising aggregation (the collection of data) and can then infer the relationship between that data and the data the user does not have access to. This is called an inference attack.



138. B. This option is not a risk, but a (probably unrealistic) benefit, so it cannot be the right answer. The other three options are all risks associated with an unmanaged patching model.

139. B. Clustering algorithms are frequently used for anomaly detection. Classifiers are helpful when trying to determine whether a binary file is malware or detect whether an e-mail is spam. Predictive machine learning models can be applied wherever historical numerical data is available and work by estimating what the value of the next data point should be, which makes them very useful for network flow analysis (e.g., when someone is exfiltrating large amounts of data from the network).

140. A. Breach and attack simulations (BAS) are automated systems that launch simulated attacks against a target environment and then generate reports on their findings. They are meant to be run regularly (even frequently) and be realistic, but not to cause any adverse effect to the target systems. They are usually a much more affordable approach than red teaming, even if you use an internal team.

141. A. Maximum tolerable downtime (MTD) is the outage time that can be endured by an organization, and the recovery time objective (RTO) is an allowable amount of downtime. The RTO value (13 hours) is smaller than the MTD value (24 hours) because the MTD value represents the time after which an inability to recover significant operations will mean severe and perhaps irreparable damage to the organization’s reputation or bottom line. The RTO assumes that there is a period of acceptable downtime. This means that a company can be out of

production for a certain period of time (RTO) and still get back on its feet. But
if the company cannot get production up and running within the MTD window,
the company is sinking too fast to properly recover.
142. C. High availability (HA) is a combination of technologies and processes that
work together to ensure that critical functions are always up and running at the
necessary level. To provide this level of high availability, a company has to have a
long list of technologies and processes that provide redundancy, fault tolerance,
and failover capabilities.

↟APPENDIX

Objective Map
All-in-One Coverage
Domain

Objective

Ch #

Heading

Domain 1: Security and Risk Management
1.1

Understand, adhere to, and promote
professional ethics

1

Professional Ethics

1.1.1

(ISC)2 Code of Professional Ethics

1

(ISC)2 Code of
Professional Ethics

1.1.2

Organizational code of ethics

1

Organizational Code of
Ethics

1.2

Understand and apply security concepts (confidentiality, integrity, and availability, authenticity and nonrepudiation)

1

Fundamental Cybersecurity Concepts and Terms

1.3

Evaluate and apply security governance principles

1

Security Governance Principles

1.3.1

Alignment of the security function to business strategy, goals, mission, and objectives

1

Aligning Security to Business Strategy

1.3.2

Organizational processes (e.g., acquisitions, divestitures, governance committees)

1

Organizational Processes

1.3.3

Organizational roles and responsibilities

1

Organizational Roles and Responsibilities

1.3.4

Security control frameworks

4

Security Control Frameworks

1.3.5

Due care/due diligence

3

Due Care vs. Due
Diligence

1.4

Determine compliance and other
requirements

3

Compliance
Requirements

1.4.1

Contractual, legal, industry standards, and
regulatory requirements

3

Contractual, Legal,
Industry Standards,
and Regulatory
Requirements

1.4.2

Privacy requirements

3

Privacy Requirements

1.5

Understand legal and regulatory issues
that pertain to information security in
a holistic context

3

Laws and Regulations

1209

B

| 1210<br>All-in-One Coverage<br>Domain | Objective | Ch # | Heading |
|---|---|---|---|
| Domain 1: Security and Risk Management | 1.5.1 | 3 | Cybercrimes and Data Breaches |
| | 1.5.2 | 3 | Licensing and Intellectual Property Requirements |
| | 1.5.3 | 3 | Import/Export Controls |
| | 1.5.4 | 3 | Transborder Data Flow |
| | 1.5.5 | 3 | Privacy |

Privacy

1.6

Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

3

Requirements for Investigations

1.7

Develop, document, and implement security policy, standards, procedures, and guidelines

1

Security Policies, Standards, Procedures, and Guidelines

1.8

Identify, analyze, and prioritize Business Continuity (BC) requirements

2

Business Continuity

1.8.1

Business Impact Analysis (BIA)

2

Business Impact Analysis

1.8.2

Develop and document the scope and the plan

2

Business Continuity

1.9

Contribute to and enforce personnel security policies and procedures

1

Personnel Security

1.9.1

Candidate screening and hiring

1

Candidate Screening and Hiring

1.9.2

Employment agreements and policies

1

Employment Agreements and Policies

1.9.3

Onboarding, transfers, and termination processes

1

Onboarding, Transfers and Termination Processes

1.9.4

Vendor, consultant, and contractor agreements and controls

1

Vendors, Consultants, and Contractors

1.9.5

Compliance policy requirements

1

Compliance Policies

1.9.6

Privacy policy requirements

1

Privacy Policies

1.10

Understand and apply risk management concepts

2

Risk Management Concepts

1.10.1

Identify threats and vulnerabilities

2

Identifying Threats and Vulnerabilities

1.10.2

Risk assessment/analysis

2

Assessing Risks

1.10.3

Risk response

2

Responding to Risks

1.10.4

Countermeasure selection and implementation

2

Countermeasure Selection and Implementation

↟Appendix B: Objective Map

1211

All-in-One Coverage
Domain

Objective

Ch #

Heading

Domain 1: Security and Risk Management
1.10.5

Applicable types of controls (e.g., preventive, detective, corrective)

2

Types of Controls

1.10.6

Control assessments (security and privacy)

2

Control Assessments

1.10.7

Monitoring and measurement

2

Monitoring Risks

1.10.8

Reporting

2

Risk Reporting

1.10.9

Continuous improvement (e.g., Risk maturity modeling)

2

Continuous Improvement

1.10.10

Risk frameworks

4

Risk Frameworks

1.11

Understand and apply threat modeling concepts and methodologies

9

Threat Modeling

1.12

Apply Supply Chain Risk Management (SCRM) concepts

2

Supply Chain Risk Management

1.12.1

Risks associated with hardware, software, and services

2

Risks Associated with Hardware, Software, and Services

1.12.2

Third-party assessment and monitoring

2

Other Third-Party Risks

1.12.3

Minimum security requirements

2

Minimum Security Requirements

1.12.4

Service level requirements

2

Service Level
Agreements

1.13

Establish and maintain a security
awareness, education, and training
program

1

Security Awareness,
Education, and Training
Programs

1.13.1

Methods and techniques to present awareness
and training (e.g., social engineering, phishing,
security champions, gamification)

1

Methods and Techniques
to Present Awareness
and Training

1.13.2

Periodic content reviews

1

Periodic Content
Reviews

1.13.3

Program effectiveness evaluation

1

Program Effectiveness
Evaluation

5

Information and Assets

Domain 2: Asset Security
2.1

Identify and classify information
and assets

2.1.1

Data classification

5

Data Classification

2.1.2

Asset classification

5

Asset Classification

2.2

Establish information and asset handling
requirements

5

Classification

2.3

Provision resources securely

5

Secure Provisioning

2.3.1

Information and asset ownership

5

Ownership

↟CISSP All-in-One Exam Guide

1212
All-in-One Coverage
Domain

| Objective | Ch # | Heading |
| --- | --- | --- |
| Domain 2: Asset Security | | |
| 2.3.2 | | Asset inventory (e.g., tangible, intangible) |
| | 5 | Inventories |
| 2.3.3 | | Asset management |
| | 5 | Managing the Life Cycle of Assets |
| 2.4 | | Manage data lifecycle |
| | 5 | Data Life Cycle |
| 2.4.1 | | Data roles (i.e., owners, controllers, custodians, processors, users/subjects) |
| | 5 | Data Roles |
| 2.4.2 | | Data collection |
| | 5 | Data Collection |
| 2.4.3 | | Data location |
| | 5 | |

Where in the World
Is My Data?

2.4.4

Data maintenance

5

Data Maintenance

2.4.5

Data retention

5

Data Retention

2.4.6

Data remanence

5

Data Remanence

2.4.7

Data destruction

5

Data Destruction

2.5

Ensure appropriate asset retention (e.g.,
End-of-Life (EOL), End-of-Support (EOS))

5

Asset Retention

2.6

Determine data security controls and
compliance requirements

6

Data Security Controls

2.6.1

Data states (e.g., in use, in transit, at rest)

6

Data States

2.6.2

Scoping and tailoring

6

Scoping and Tailoring

2.6.3

Standards selection

6

Standards

2.6.4

Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))

6

Data Protection Methods

Domain 3: Security Architecture and Engineering
3.1

Research, implement and manage engineering processes using secure design principles

9

Secure Design Principles

3.1.1

Threat modeling

9

Threat Modeling

3.1.2

Least privilege

9

Least Privilege

3.1.3

Defense in depth

9

Defense in Depth

3.1.4

Secure defaults

9

Secure Defaults

3.1.5

Fail securely

9

Fail Securely

3.1.6

Separation of Duties (SoD)

9

Separation of Duties

3.1.7

Keep it simple

9

Keep It Simple

3.1.8

Zero Trust

9

Zero Trust

3.1.9

Privacy by design

9

Privacy by Design

↟Appendix B: Objective Map

1213
All-in-One Coverage
Domain

Objective

Ch #

Heading

Domain 3: Security Architecture and Engineering
3.1.10

Trust but verify

9

Trust But Verify

3.1.11

Shared responsibility

9

Shared Responsibility

3.2

Understand the fundamental concepts of
security models (e.g., Biba, Star Model,
Bell-LaPadula)

9

Security Models

3.3

Select controls based upon systems security requirements

9

Security Requirements

3.4

Understand security capabilities of Information Systems (IS) (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

9

Security Capabilities of Information Systems

3.5

Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

7

General System Architectures

3.5.1

Client-based systems

7

Client-Based Systems

3.5.2

Server-based systems

7

Server-Based Systems

3.5.3

Database systems

7

Database Systems

3.5.4

Cryptographic systems

8

Cryptosystems

3.5.5

Industrial Control Systems (ICS)

7

Industrial Control
Systems

3.5.6

Cloud-based systems (e.g., Software as a
Service (SaaS), Infrastructure as a Service
(IaaS), Platform as a Service (PaaS))

7

Cloud-Based Systems

3.5.7

Distributed systems

7

Distributed Systems

3.5.8

Internet of Things (IoT)

7

Internet of Things

3.5.9

Microservices

7

Microservices

3.5.10

Containerization

7

Containerization

3.5.11

Serverless

7

Serverless

3.5.12

Embedded systems

7

Embedded Systems

3.5.13

High-Performance Computing (HPC) systems

7

High-Performance
Computing Systems

3.5.14

Edge computing systems

7

Edge Computing
Systems

3.5.15

Virtualized systems

7

Virtualized Systems

3.6

Select and determine cryptographic
solutions

8

Cryptography Definitions
and Concepts

3.6.1

Cryptographic life cycle (e.g., keys, algorithm selection)

8

Cryptographic Life Cycle

↟CISSP All-in-One Exam Guide

1214

All-in-One Coverage Domain

Objective

Ch #

Heading

Domain 3: Security Architecture and Engineering

3.6.2

Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)

8

Cryptographic Methods

3.6.3

Public Key Infrastructure (PKI)

8

Public Key Infrastructure

3.6.4

Key management practices

8

Key Management

3.6.5

Digital signatures and digital certificates

8

Digital Signatures
Digital Certificates

3.6.6

Non-repudiation

8

Cryptosystems

3.6.7

Integrity (e.g., hashing)

8

Cryptosystems

3.7

Understand methods of cryptanalytic attacks

8

Integrity

3.7.1

Brute force

8

Brute Force

3.7.2

Ciphertext only

8

Ciphertext-Only Attacks

3.7.3

Known plaintext

8

Known-Plaintext Attacks

3.7.4

Frequency analysis

8

Frequency Analysis

3.7.5

Chosen ciphertext

8

Chosen-Ciphertext
Attacks

3.7.6

Implementation attacks

8

Implementation Attacks

3.7.7

Side-channel

8

Side-Channel Attacks

3.7.8

Fault injection

8

Fault Injection

3.7.9

Timing

8

Side-Channel Attacks

3.7.10

Man-in-the-Middle (MITM)

8

Man-in-the-Middle

3.7.11

Pass the hash

8

Replay Attacks

3.7.12

Kerberos exploitation

17

Weaknesses of Kerberos

3.7.13

Ransomware

8

Ransomware

3.8

Apply security principles to site and facility design

10

Security Principles

3.9

Design site and facility security controls

10

Site and Facility Controls

3.9.1

Wiring closets/intermediate distribution facilities

10

Distribution Facilities

3.9.2

Server rooms/data centers

10

Data Processing Facilities

3.9.3

Media storage facilities

10

Media Storage

3.9.4

Evidence storage

10

Evidence Storage

3.9.5

Restricted and work area security

10

Restricted Areas

↟Appendix B: Objective Map

1215
All-in-One Coverage
Domain

Objective

Ch #

Heading

Domain 3: Security Architecture and Engineering
3.9.6

Utilities and Heating, Ventilation, and Air Conditioning (HVAC)

10

Utilities

3.9.7

Environmental issues

10