1. A:internet of things
2. a: physical location of stored data
3. c: Anonymization
4. b: potential customer
5. b: PaaS
6. d: the industry vertical
7. b: certification
8. d: none
9. d: both cloud provider and cloud customer
10. d: code signing does not ensure that the code is free from bug
11. d: web application firewall (WAF)
12. d: Authorization
13. d: validating and escaping all untrusted info sent to server
14. d: sensitivity related to confidentiality and criticality related to availabilty
15. a
16. c: 52.60
17. d: impact is low and probability is low
18. c: column level
19. a:
20. b: 24
21. a: security
22. a:minimal management effort and shared resource
23. b: protect the CIA
24. a: est responsibility and accountability
25. a: saas
26. a: PCI DSS
27. c: mitigate risk and reduce potential lost
28. a :private
29. b: data residency is in another county
30. a: user accountability for the action on the system
31. a: bare-metal hypervisor
32. c: increase data privacy
33. c: comply with the EU GDPR requirement
34. c: cross site scripting (XSS)
35. c; service level agreement
36. b; zero day exploit bc it tries to exploit unknown or undisclosed vulnerability
37. a : requirement gatherign, desig
38. a: physical security
39. a: confidentiality
40. c: when a door opens , the air goes out
41. a; pseudonymization
42. b: hight humidity causes corrosion and low causes static electricity
43. c: application level encryption
44. b: gaps analysis
45. d: authorization
46. c: structured and unstructured
47. b: makes it difficult to perform database functions like searches and indexing
48. b: false positive and false negative
49. b: encryption
50. b: RTO defines how long to recover and RPO defines how far back
51. a: data controller
52. a: highly motivated, skilled and patient attackers
53. c: use primarily for entrapment
54. b: determine proper handling procedures
55. b: increased security
56. b: association of unrelated third party org that shares info based on a single sign-on
57. c: password reuse attack (two factor authentication
58. a: time to run scans
59. b: homomorphic encryption
60. a: cloud access security broker (CASB)
61. b: component level,system level,and penetration testing to validate the system security
62. b: define objective , define scope, conduct audit , lesson learned
63. c: the budget for security testing is limited or non-existent
64. a: the organization’s risk culture
65. a; power down the complete sys and all the peripheral devices
66. a: 80.6
67. b: the best possible safeguard should always be implemented regardless of cost
68. a; due care
69. a: hot aisle containment
70. a: minimize the degree of contamination to the scene and evidence
71. a: value of database
72. c: event are anything that can occur within the system , while incidents are unscheduled events
73. c: data in use
74. b: preventive controls sometimes prevent a desired outcome
75. b: when the cost of countermeasure is more than the asset value
76. b: chain of custody
77. d: review the code
78. d: cloud production environment ; on -premises BCDR environment
79. d: 7
80. a: create
81. c: apply security patches as they are released
82. b: asymmetric and symmetric
83. c: logs should not contain activities of all high privileged accounts
84. b: data owner
85. a: SOAP
86. a: BC/DR
87. d: IaaS private
88. d: payment card industry data security standard (PCI DSS)
89. c: availability
90. b) virtualization sprawl
91. d: security misconfiguration
92. b: it will cause additional processing overhead and delay
93. a: tokenization or masking
94. d: disclosure
95. a: ISO/IEC 27018
96. b: halon has ozone depleting properties
97. d: all of the above
98. c: system efficiency, security expenses , and information protection
99. b: ensure that the evidence has been accounted for
100. d; data processor
101. d: the new key encrypted using the private key of X is transmitted from X to Y
102. b: there is no one-size fits-all solution
103. b: legal hold
104. b: system availability
105. c: tier III
106. c: measured service
107. a: waterfall model
108. b: comprehensive documentation over working software
109. a: lack of formal documentation or comprehensive planning that could impact software security
110. b: heuristics-based rules
111. a: sold as standalone device
112. a: relying party
113. d: the service provider it consumes token generated by the identity provider
114. d: crypto shredding
115. b: IDS can easily distinguish a malicious payload in encrypted traffic
116. a: in real time
117. b: Anonymization
118. d: problem management
119. b: information right management
120. d: recovery time objective (RTO)
121. b: a higher MTBF and a lower MTTR
122. b: recovery service level (RSL)
123. b: private cloud
124. d: retention periods, data fomats, data security , storage method, and data retrieval procedure
125. c: reclassify