

CISSP 125 Question Answers and References

Question	Answer	Content	Where Answers found
1	B	What is Confidentiality related to	10 and others
2	B	Building Security into an Application	722
3	C	Releasing a product and making it secure	Policy is almost always right
4	A	Security Officer Administrative Structures	15-17
5	C	What does Governance involve?	17, 20
6	C	Intellectual Property and Contract Law	24
7	D	International Encryption Export Restrictions	25
8	A	OECD Guidelines on Privacy	25, 26
9	B	Skimming vs. spoofing in access control	453
10	B	RTO and RTO and End of Disaster actions	42, 43
11	C	Employee Termination Activities	48
12	C	ARO, SLE, AV, ALE terms	58, 59
13	D	Application Development Scenario -- prevention	Only answer that makes sense
14	B	Corrective Activities	68-70
15	D	White/Black Box testing Damage	543, 547
16	A	Social Engineering Examples	86, 87, 420
17	B	Security Policy Change Reasons	PDCA p83 and common sense
18	B	Purpose of Information Classification	111-113
19	C	Statements about Information Categorization	111-113
20	D	What's missing from information polices? Database Scenario Questions 21-23 Best way to make sure data only available to those with need	112 and remember "missing"
21	D	to know	750, 751
22	C	PCI-DSS Data Storage security	111, 224 , 854
23	D	HIPAA Data Storage Security	21, 358
24	D	Owner vs. data custodian	81, 128, 129
25	D	Data Life Cycle Issues	135
26	A	Destroying cloud stored data and data remanence	140, 143
27	D	Best way to delete data on a SSD	142, 143
28	A	How should a company retain data?	Reverse Logic
29	D	Reasons to adopt a cyber-security framework Best way to protect confidential data on thumb drive to	166 and references
30	C	prevent loss	172
31	C	What is the European "Right to be Forgotten"?	180
32	B	CMM-DEV Levels in an organization	196, 606, 728, 729
33	C	Memory protection options	200, 201
34	A	ESA Advantages and Disadvantages	204, 205
35	C	Confidentiality Models	209 - 213
36	B	Security Lattice Models	211
37	A	Security Models: Which is which?	209 - 213
38	D	Product Evaluation Models	216-219
39	C	PCI-DSS Implementation Issues	224, reference on p 339
40	B	CPU states	p 227
41	D	Dangerous malware that hides files	421, 534, 538
42	D	Diskless workstations vs. thin clients	235, 359
43	C	How are passwords stored	493
44	B	Suggestions from reading medical records Database terms, aggregation, data mining, instantiation,	xiv, 136, 173, 239
45	C	Metadata	239

CISSP 125 Question Answers and References

Question	Answer	Content	Where Answers found
46	D	Grid Computing	239, 241
47	A	Cloud Computing Countermeasures	242, 243
48	C	What does a Digital Signature provide?	244, 247
49	B	SSL/TLS Session key	368, graph on p 400
50	C	SSL Session Key	400
51	D	SSL Handshake	400
52	B	Plaintext and Ciphertext attacks	306, 307
53	D	Digital Signature Creation Steps	Xii, Xiv, 10, 244, 247, 290. 299, 853
54	C	Transposition Ciphers	252, 253
55	B	What is IAAA in access control?	448, 449
56	D	International Copyright agreement agencies	103, 300
57	D	Closed Circuit Television is what kind of control?	70
58	A	What is a compensating control?	66, 67, 70
59	B	CPTED components	315
60	A	Glass Types and advantages /disadvantages	316
61	D	Dangers when something catches fire	318, 327, 328,
62	A	ODBC Issues	745
63	B	Routers and Router tables and the OSI Layers	xvi, xvii, 348, 349
64	C	SDLC Phases	770
65	B	IPSEC Transport Level Key Exchange options	388 - 390
66	D	TCP Flag Bits and their uses	350, 418, 419 diagram
67	A	SCADA systems and their security	278, 279, 360
68	C	Multi Protocol Label Switching features	345, 362, 399, 434
69	D	Wireless solutions for different type networks	364
70	C	Repeaters vs. Amplifiers	374, 379
71	B	IP Private Address Pool RFC 1918	355, 380
72	A	Using IPSEC with RFC 1918 Pools	388 - 390
73	C	Differences in CSMACD and CSMA/CA in LANs	397, 398
74	B	Benefits of Cable Modems vs. DSL	405, 406
75	C	Software Defined Networking Layers	406 - 409
76	D	Private VLAN PVLAN types	412 - 413
77	C	What is Enumeration?	419 - 421
78	C	Least likely attack on modern networking devices?	356, 433
79	B	Which is the least secure method of identification	450, 515, 610, 705
80	D	Successfully preventing unauthorized access	88, 449 - 454
81	A	Which access control type is done by the operating system?	496 - 500
82	C	"Clearances" in Access control systems	498, 611, 613
83	D	Who defines corporate data classifications?	10, 112, 113
84	D	Best way to prevent personnel access	325, 702 - 704
85	A	Requires two keys to be turned simultaneously to gain access	293
86	A	In a DAC environment, Need to know is part of?	110
87	A	Foreign and Primary keys in a database system	742
88	C	Database Models	739-741
89	C	In a Non DAC environment, who makes the classification decisions?	500, 612 Notes unclear here
90	C	Where is IDaaS essential?	486 - 488
91	C	What does a copyright protect?	24, 100, 115

CISSP 125 Question Answers and References

Question	Answer	Content	Where Answers found
92	B	Surrender keys	xviii, 613, 618
93	B	Identity and Access Management lifecycle Steps	xviii, 613, 618
94	B	Software Development Methods	734-736
95	C	Most common consideration for logging activities	532, 533, 537 - 539
96	B	Common Operating System Log Entries	532, 533, 537 - 539
97	C	A Security Provider's Security Controls	568, 569, 570, 571
98	B	What is an Incident Scene?	582 - 585
99	B	What are the SWGDE principles	722, 726, 728
100	C	Certification vs. Accreditation in software Scenario on Incident Investigation	582 - 585
101	C	What are the first steps in setting up a SIEM system.	595, 623, 632, 633
102	B	What to do with large log files? After identifying a suspect, you add additional logging to cover	644, 646, 712, 758, 821
103	D	every action that person takes. What can your organization do if law enforcement takes over	590 - 592
104	D	an investigation?	590 - 592
105	A	What is Deep-packet inspection?	597 - 599
106	D	What is the least effective way to hide data in transit?	526
107	C	What do Configuration Management systems track?	533, 563, 570
108	C	Where should Separation of Duties be implemented?	611, 612
109	D	What is the Data Owner responsible for?	613, 614
110	D	What is in a Service Level Agreement?	615, 616
111	B	What is data Remanence?	121, 140, 143, 182, 622, 851
112	B	What are well known incidence response frameworks?	162 - 170
113	B	An incident vs. an Event	849
114	C	What is a network firewall?	379
115	C	Which vulnerability should you patch last?	199, 392, 787, 788,
116	C	Which BCP statement is true?	675, 680, 688
117	B	What does "work for hire entail?"	49, 115, 299
118	D	What types of controls are used in different circumstances?	66-70, 292, 849 Not in notes, but answer can be learned by deduction.
119	C	What is the main advantage of the new EMV credit cards?	deduction.
120	D	What should a fire door be made of?	703
121	A	Active vs. Passive Intrusion sensors	695, 860
122	B	What is a hardened hinge?	702, 703
123	B	What makes fireproof safes safe?	A matter of deduction.
124	C	What is in SLC and not in SDLC? What are the components of functional design	722
125	A	documentation?	722 - 725