Answers

Here are the answers to the questions:

Q	***Answers***	***Assessment Criteria***
1	**B.**	To prevent crime
2	**C.**	Criminal investigations
3	**C.**	Public law enforcement is funded by taxpayers
4	**D.**	They help security personnel avoid violent confrontations
5	**A.**	To identify potential threats and vulnerabilities
6	**C.**	Access control systems
7	**B.**	To establish rules and guidelines for protecting assets
8	**C.**	Cyberattacks
9	**A.**	To identify security vulnerabilities and risks
10	**A.**	Passwords
11	**C.**	Encryption
12	**B.**	To provide information for criminal investigations
13	**D.**	All of the above
14	**A.**	A user using a weak password
15	**A.**	To deter crime
16	**C.**	Unsecured Wi-Fi networks
17	**D.**	All of the above
18	**A.**	Security officers have more training than security guards
19	**A.**	To prevent unauthorized access to a facility
20	**C.**	Unsecured Wi-Fi networks
21	**B.**	To design and implement security systems and policies
22	**B.**	To establish rules and guidelines for protecting assets
23	**A.**	Access control systems
24	**A.**	To identify potential threats and take action to prevent violence from occurring
25	A.	To educate employees on security policies and procedures
26	A.	Regular backups of data
27	A.	To oversee the daily operations of a security team
28	A.	Providing conflict resolution training to employees
29	A.	To monitor a facility for security breaches
30	D.	All of the above
31	A.	Active security measures involve physical security devices, while passive security measures involve policies and procedures
32	A.	To identify potential security threats and vulnerabilities

33	A.	Access control systems
34	A.	To provide first aid to injured parties
35	D.	None of the above
36	D.	All of the above
37	A.	To evaluate the effectiveness of a security program
38	A.	Providing conflict resolution training to employees
39	D.	All of the above
40	A.	To establish rules and guidelines for protecting assets
41	A.	Regular backups of data
42	A.	To monitor for suspicious behaviour and packages
43	A.	To document security incidents for future reference
44	B.	Providing fraud awareness training to employees
45	B.	To prevent accidents from occurring in the first place
46	A.	Shredding documents containing sensitive information
47	D.	All of the above
48	A.	Installing alarm systems
49	B.	To investigate harassment claims
50	A.	To identify potential security threats and vulnerabilities
51	A.	Installing surveillance cameras
52	B.	To coordinate with emergency responders
53	B.	Restricting access to sensitive information
54	A.	To identify potential security threats and vulnerabilities
55	B.	Providing self-defence training to employees
56	B.	To investigate reports of product tampering
57	E.	To provide a framework for responding to security incidents
58	B.	Restricting access to sensitive information
59	C.	To prevent terrorism from occurring in the first place
60	B.	Providing self-defence training to employees
61	D.	To evaluate the effectiveness of a security program
62	B.	Restricting access to sensitive information

63	C.	To investigate reports of theft
64	D.	To control access to sensitive areas
65	C.	To investigate reports of discrimination
66	B.	Restricting access to sensitive information
67	A.	To establish security policies and procedures
68	B.	Restricting access to sensitive information.
69	C.	Use of excessive force.
70	C.	Maintaining public order and safety.