Memory Tables Answer Key

Chapter 1

As part of determining how critical an asset is, you need to understand the following terms:

- **Maximum tolerable downtime (MTD):** The maximum amount of time that an organization can tolerate a single resource or function being down. This is also referred to as maximum period time of disruption (MPTD).
- **Mean time to repair (MTTR):** The average time required to repair a single resource or function when a disaster or disruption occurs.
- **Mean time between failure (MTBF):** The estimated amount of time a device will operate before a failure occurs. This amount is calculated by the device vendor. System reliability is increased by a higher MTBF and lower MTTR.
- **Recovery time objective (RTO):** The shortest time period after a disaster or disruptive event within which a resource or function must be restored to avoid unacceptable consequences. RTO assumes that an acceptable period of downtime exists. RTO should be smaller than MTD.
- **Work recovery time (WRT):** The difference between RTO and MTD, which is the remaining time that is left over after the RTO before reaching the maximum tolerable.
- **Recovery point objective (RPO):** The point in time to which the disrupted resource or function must be returned.

Table 1-4 Administrative (Management) Controls

Administrative (Management) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Personnel procedures						X	
Security policies				X	X	X	
Monitoring			X				
Separation of duties						X	
Job rotation	X		X				
Information classification						X	
Security awareness training						X	
Investigations			X				
Disaster recovery plan						X	X
Security reviews			X				
Background checks			X				
Termination		X					
Supervision	X						

Table 1-5 Logical (Technical) Controls

Logical (Technical) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Password						X	
Biometrics						X	
Smart cards						X	
Encryption						X	
Protocols						X	

Logical (Technical) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Firewalls						X	
IDS			X				
IPS						X	
Access control lists						X	
Routers						X	
Auditing			X				
Monitoring			X				
Data backups							X
Antivirus software						X	
Configuration standards					X		
Warning banners				X			
Connection isolation and termination		X					

Table 1-6 Physical Controls

Physical (Technical) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Fencing				X		X	
Locks						X	
Guards			X			X	
Fire extinguisher		X					
Badges						X	
Swipe cards						X	
Dogs			X			X	
Man traps						X	

Physical (Technical) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Biometrics						X	
Lighting				X			
Motion detectors			X				
CCTV	X		X			X	
Data backups							X
Antivirus software						X	
Configuration standards					X		
Warning banner				X			
Hot, warm, and cold sites							X

Chapter 2

Table 2-1 RAID

RAID Level	Min. Number of Drives	Description	Strengths	Weaknesses
RAID 0	2	Data striping without redundancy	Highest performance	No data protection; one drive fails, all data is lost
RAID 1	2	Disk mirroring	Very high performance; very high data protection; very minimal penalty on write performance	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required
RAID 3	3	Byte-level data striping with dedicated parity drive	Excellent performance for large, sequential data requests	Not well-suited for transaction-oriented network applications; single parity drive does not support multiple, simultaneous read and write requests

RAID Level	Min. Number of Drives	Description	Strengths	Weaknesses
RAID 5	3	Block-level data striping with distributed parity	Best cost/performance for transaction-oriented networks; very high performance, very high data protection; supports multiple simultaneous reads and writes; can also be optimized for large, sequential requests	Write performance is slower than RAID 0 or RAID 1
RAID 10	4	Disk striping with mirroring	High data protection, which increases each time to add a new striped/mirror set	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required

Table 2-2 Confidentiality, Integrity, and Availability Potential Impact Definitions

CIA Tenet	Low	Moderate	High
Confidentiality	Unauthorized disclosure will have limited adverse effect on the organization.	Unauthorized disclosure will have serious adverse effect on the organization.	Unauthorized disclosure will have severe adverse effect on the organization.
Integrity	Unauthorized modification will have limited adverse effect on the organization.	Unauthorized modification will have serious adverse effect on the organization.	Unauthorized modification will have severe adverse effect on the organization.
Availability	Unavailability will have limited adverse effect on the organization.	Unavailability will have serious adverse effect on the organization.	Unavailability will have severe adverse effect on the organization.

Chapter 3

Table 3-4 Symmetric Algorithm Strengths and Weaknesses

Strengths	Weaknesses
1,000 to 10,000 times faster than asymmetric algorithms	Number of unique keys needed can cause key management issues
Hard to break	Secure key distribution critical
Cheaper to implement than asymmetric	Key compromise occurs if one party is compromised, thereby allowing impersonation

Table 3-5 Asymmetric Algorithm Strengths and Weaknesses

Strengths	Weaknesses
Key distribution is easier and more manageable than with symmetric algorithms	More expensive to implement than symmetric algorithms
Key management is easier because the same public key is used by all parties	1,000 to 10,000 times slower than symmetric algorithms

Table 3-6 Symmetric Algorithms Key Facts

Algorithm Name	Block or Stream Cipher?	Key Size	Number of Rounds	Block Size
DES	Block	64 bits (effective length 56 bits)	16	64 bits
3DES	Block	56, 112, or 168 bits	48	64 bits
AES	Block	128, 192, or 256 bits	10, 12, or 14 (depending on block/key size)	128, 192, or 256 bits
IDEA	Block	128 bits	8	64 bits
Skipjack	Block	80 bits	32	64 bits
Blowfish	Block	32–448 bits	16	64 bits
Twofish	Block	128, 192, or 256 bits	16	128 bits
RC4	Stream	40–2,048 bits	Up to 256	N/A
RC5	Block	Up to 2,048	Up to 255	32, 64, or 128 bits
RC6	Block	Up to 2,048	Up to 255	32, 64, or 128 bits

Table 3-7 Protection Requirements for Cryptographic Keys

Key Type	Security Service	Security Protection	Period of Protection
Private signature key	Source authentication Integrity authentication Support nonrepudiation	Integrity Confidentiality	From generation until the end of the cryptoperiod
Public signature verification key	Source authentication Integrity authentication Support nonrepudiation	Integrity	From generation until no protected data needs to be verified

Key Type	Security Service	Security Protection	Period of Protection
Symmetric authentication key	Source authentication Integrity authentication	Integrity Confidentiality	From generation until no protected data needs to be verified
Private authentication key	Source authentication Integrity authentication	Integrity Confidentiality	From generation until the end of the cryptoperiod
Public authentication key	Source authentication Integrity authentication	Integrity	From generation until no protected data needs to be authenticated
Symmetric data encryption/ decryption key	Confidentiality	Integrity Confidentiality	From generation until the end of the lifetime of the data or the end of the cryptoperiod, whichever comes later
Symmetric key-wrapping key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or until no wrapped keys require protection, whichever is later
Symmetric RBG key	Support	Integrity Confidentiality	From generation until replaced
Symmetric master key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or the end of the lifetime of the derived keys, whichever is later
Private key-transport key	Support	Integrity Confidentiality	From generation until the end of the period of protection for all transported keys
Public key-transport key	Support	Integrity	From generation until the end of the cryptoperiod
Symmetric key-agreement key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or until no longer needed to determine a key, whichever is later
Private static key-agreement key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or until no longer needed to determine a key, whichever is later

Key Type	Security Service	Security Protection	Period of Protection
Public static key-agreement key	Support	Integrity	From generation until the end of the cryptoperiod or until no longer needed to determine a key, whichever is later
Private ephemeral key-agreement key	Support	Integrity Confidentiality	From generation until the end of the key-agreement process; after the end of the process, the key is destroyed
Public ephemeral key-agreement key	Support	Integrity	From generation until the key-agreement process is complete
Symmetric authorization keys	Authorization	Integrity Confidentiality	From generation until the end of the cryptoperiod of the key
Private authorization key	Authorization	Integrity Confidentiality	From generation until the end of the cryptoperiod of the key
Public authorization key	Authorization	Integrity	From generation until the end of the cryptoperiod of the key

Table 3-8 Fire Extinguisher Classes

Class	Type of Fire
Class A	Ordinary combustibles
Class B	Flammable liquids, flammable gases
Class C	Electrical equipment
Class D	Combustible metals
Class K	Cooking oil or fat

Chapter 4

Table 4-1 Common TCP/UDP Port Numbers

Application Protocol	Transport Protocol	Port Number
Telnet	TCP	23
SMTP	UDP	25
HTTP	TCP	80
SNMP	TCP and UDP	161 and 162
FTP	TCP and UDP	20 and 21
FTPS	TCP	989 and 990
SFTP	TCP	22
TFTP	UDP	69
POP3	TCP and UDP	110
DNS	TCP and UDP	53
DHCP	UDP	67 and 68
SSH	TCP	22
LDAP	TCP and UDP	389
NetBIOS	TCP and UDP	137 (TCP), 138 (TCP), and 139 (UDP)
CIFS/SMB	TCP	445
NFSv4	TCP	2049
SIP	TCP and UDP	5060
XMPP	TCP	5222
IRC	TCP and UDP	194
RADIUS	TCP and UDP	1812 and 1813
rlogin	TCP	513
rsh and RCP	TCP	514
IMAP	TCP	143
HTTPS	TCP and UDP	443
RDP	TCP and UDP	3389
AFP over TCP	TCP	548

Table 4-2 Classful IP Addressing

Class	Range	Mask	Initial Bit Pattern of First Octet	Network/Host Division
Class A	0.0.0.0–127.255.255.255	255.0.0.0	01	net.host.host.host
Class B	128.0.0.0–191.255.255.255	255.255.0.0	10	net.net.host.host
Class C	192.0.0.0–223.255.255.255	255.255.255.0	11	net.net.net.host
Class D	224.0.0.0–239.255.255.255	Used for multicasting		
Class E	240.0.0.0–255.255.255.255	Reserved for research		

Table 4-3 Private IP Address Ranges

Class	Range
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

Table 4-4 WPA and WPA2

Variant	Access Control	Encryption	Integrity
WPA Personal	Preshared key	TKIP	Michael
WPA Enterprise	802.1X (RADIUS)	TKIP	Michael
WPA2 Personal	Preshared key	CCMP, AES	CCMP
WPA2 Enterprise	802.1X (RADIUS)	CCMP, AES	CCMP

Table 4-5 Twisted-Pair Categories

Name	Maximum Transmission Speed
Cat3	10 Mbps
Cat4	16 Mbps
Cat5	100 Mbps
Cat5e	100 Mbps

Name	Maximum Transmission Speed
Cat6	1 Gbps
Cat6a	10 Gbps
Cat7	10 Gbps
CaT7a	10 Gbps; 40 Gbps (50 meters); 100 Gbps (15 meters)

Table 4-6 Selected Fiber Specifications

Standard	Distance
100Base-FX	Maximum length is 400 meters for half-duplex connections (to ensure collisions are detected) or 2 kilometers for full-duplex.
1000Base-SX	550 meters
1000Base-LX	Multi-mode fiber (up to 550 meters) or single-mode fiber (up to 2 kilometers; can be optimized for longer distances, up to 10 kilometers)
10GBase-LR	10 kilometers
10GBase-ER	40 kilometers

Table 4-7 Ethernet Implementations

Ethernet Type	Cable Type	Speed
10Base2	Coaxial	10 Mbps
10Base5	Coaxial	10 Mbps
10BaseT	Twisted pair	10 Mbps
100BaseTX	Twisted pair	100 Mbps
1000BaseT	Twisted pair	1000 Mbps
1000BaseX	Fiber	1000 Mbps
10GBaseT	Twisted pair	10 Gbps