CompTIA Security+ Study Guide SY0-701

Study online at https://quizlet.com/_eby0w6

The organization that Chris works for has disabled automatic updates. What is the most common reason for disabling automatic updates for organizational systems?	C. To avoid issues with problematic patches and updates
Which of the following is the least volatile according to the forensic order of volatility?	B. Logs
Ed wants to trick a user to connecting to his evil twin access point (AP). What type of attack should he conduct to increase his chances of the user connecting to it?	A. A dissociation attack
What term is used to describe wireless site surveys that show the relative power of access points on a diagram of the building or facility?	D. Heatmaps
What hardware device is used to creae the hardware root of trust for modern desktops and laptops?	D. The TPM
Angela wants to prevent users in her organization from changing their passwords repeatedly so that they cannot reuse their current password. What two password security settings does she need to implement to make this occur?	A. Set a password history and a minimum password age
Chris wants to establish a backup site that is fully ready to take over for full operations for his organization at any time. What type of site should he set up?	C. A hot site
Which of the following is not a common constraint of embedded and specialized systems?	B. Overly complex firewall settings
Gary is reviewing his systems SSH logs and sees logins for the user named "Gary" with passwords like password1, password2,...,PassworD. What type of attack has Gary discovered?	A. A dictionary attack
Kathleen wants to set up a system that allows access into a high-security zone from a low-security zone. What type of solution should she configure?	D. A jump server
Derek's organization is worried about a disgruntled employee publishing sensitive business information. What type of threat should Derek work to protect against?	C. Insider threats
Jeff is concerned about the effects that a ransomware attack might have on his organization and is designing a backup methodology that would allows the organization to quickly restore after such an attack. What type of control is Jeff implementing?	A. Corrective
Samantha is investigating a cybersecurity incident where an internal user used his computer to participate in a denial of service attack against a third party. What type of policy was most likely violated?	C. AUP (acceptable use policy)
Jean recently completed the user acceptance testing process and is getting her code ready to deploy. What environment should house her code before it is release for use?	D. Staging
Oren obtained a certificate for his domain covering *. acmewidgets.net. Which one of the following domains would not be covered by this certificate? A. www.acmewidgets.net B. acmewidgets.net C. test.mail.acmewidgets.net D. mobile.acmewidgets.net	C. test.mail.acmewidgets.net
Richard is sending a message to Grace and would like to apply a digital signature to the message before sending it. What key should he use to create the digital signature?	

A. Richard's private key B. Richard's public key C. Grace's Private Key D. Grace's public key	A. Richard's private key
Andrew is workng with his financial team to purchase a cyber-security insurance policy to cover the financial impact of a data breach. What type of risk management strategy is he using?	B. Risk transference
Shelly is writing a document that describes the steps that incident response teams will follow upon first notice of a potential incident. What type of document is she creating?	C. Procedure
Rob has created a document that describes how staff in his organization can use organizationally owned devices, including if and when personal use is allowed. What type of policy has Rob created?	B. An acceptable use policy
Matt is updating the organization's threat assessment process. What category of control is Matt implementing?	D. Managerial
Jade's organization recently suffered a security breach that affected stored credit card data. Jade's primary concern is the fact that the organization is subject to sanctions for violating the provisions of the Payment Card Industry Data Security Standard. What category of risk is concerning Jade?	B. Compliance
Chris is responding to a security incident that compromised one of his organization's web servers. He believes that the attackers defaced one or more pages on the website. What cybersecurity objective did this attack violate?	C. Integrity
Tonya is concerned about the risk an attacker will attempt to gain access to her organization's database server. She is searching for a control that would discourage the attacker from attempting to gain access. What type of security control is she seeking to implement?	D. Deterrent
Greg is implementing a data loss prevention system. He would like to ensure that it protects against transmissions of sensitive information by guests on his wireless network. What DLP technology would best meet this goal? A. Watermarking B. Pattern recognition C. Host-based D. Network-based	D. Network-based
What term describes data that is being sent between two systems over a network connection?	B. Data in transit
Tina is tuning her organization's intrusion prevention system to prevent false positive alerts. What type of control is Tina implementing?	A. Technical control
Which one of the following is not a common goal of a cybersecurity attacker?	D. Allocation
Tony is reviewing the status of his organization's defenses against a breach of their file server. He believes that a compromise of the file server could reveal information that would prevent the company from continuing to do business. What term best describes the risk that Tony is considering? A. Strategic B. Reputational C. Financial D. Operational	A. Strategic
Which of the following data elements is not commonly associated with identity theft?	C. Frequent flier number

What term best describes an organization's desired security state?	A. Control objectives
What technology uses mathematical algorithms to render information unreadable to those lacking the required key?	D. Data encryption
Greg recently conducted an assessment of his organization's security controls and discovered a potential gap: the organization does not use full-disk encryption on laptops. What type of control gap exists in this case?	D. Preventive
What compliance regulation most directly affects the operations of a health-care provider?	A. HIPAA
Nolan is writing an after action report on a security breach that took place in his organization. The attackers stole thousands of customer records from the organization's database. What cybersecurity principle was most impacted in this breach?	C. Confidentiality
Which one of the following objectives is not one of the three main objectives that information security professionals must achieve to protect their organizations against cyber security threats?	B. Nonrepudiation
Which of the following data protection techniques is reversible when conducted properly?	A. Tokenization
Which one of the following statements is not true about compensating controls under PCI DSS?	A. Controls used to fulfill one PCI DSS requirement may not be used to compensate for the abscense of a control to meet another requirement
Which of the following measures is not commonly used to assess threat intelligence?	B. Detail
Which one of the following motivations is most commonly attributed to hacktivists?	C. Political and philosophical beliefs
Kolin is a penetration tester who works for a cybersecurity company. His firm was hired to conduct a penetration test against a health-care system, and Kolin is working to gain access to the systems belonging to a hospital in that system. What term best describes Kolin's work?	A. Authorized hacker
Which one of the following attackers is most likely to be associated with an APT?	A. Nation-state actor
Which organization did the U.S. government help create to share knowledge between organizations in specific verticals?	D. ISACs
Which of the following threat actors typically has the greatest access to resources?	A. Nation-state actors
Of the threat vectors shown here, which one is most commonly exploited by attackers who are at a distant location?	A. Email
Which of the following is the best example of a hacktivist group?	D. Anonymous
What type of assessment is particularly useful for identifying insider threats?	A. Behavioral
Cindy is concerned that her organization may be targeted by a supply chain attack and is conducting a review of all of her vendor and supplier partners. Which one of the following organizations is least likely to be the conduit for a supply chain attack?	D. Talent provider
Greg believes that an attacker may have installed malicious firmware in a network device before it was provided to his organization by the supplier. What type of threat vector best describes this attack?	A. Supply chain
Ken is conducting threat research on Transport Layer Security (TLS) and would like to consult the authoritative reference for the protocol's technical specification. What resource would best meet his needs?	B. Internet RFCs

Wendy is scanning cloud-based repositories for sensitive information. Which one of the following should concern her most, if discovered in a public repository?	C. API keys
Which one of the following threat research tools is used to visually display information about the location of threat actors?	A. Threat map
Vince recently received the hash values of malicious software that several other firms in his industry found installed on their systems after a compromise. What term best describes this information?	B. IoC
Ursula recently discovered that a group of developers are sharing information over a messaging tool provided by a cloud vendor but not sanctioned by her organization. What term best describes this use of technology?	A. Shadow IT
Tom's organization recently learned that the vendor is discontinuing support for their customer relationship management (CRM) system. What should concern Tom the most from a security perspective? A. Unavailability of future patches B. Lack of technical support C. Theft of customer information D. Increased costs	A. Unavailability of future patches
Which one of the following information sources would not be considered an OSINT source?	C. Port scans (Open Source Intelligence)
Edward Snowden was a government contractor who disclosed sensitive government documents to journalists to uncover what he believed were unethical activities. Which one of the following terms best describe Snowden's activities (Choose two.)	A. Insider, C. Hacktivist
Ryan wants to prevent logic bombs created by insider threats from impacting his organization. What technique will most effectively limit the likelihood of logic bombs being put in place?	B. Using a code review process
Yasmine believes that her organization may be dealing with an advanced rootkit and wants to write IoC definitions for it. Which of the following is not likely to be a useful IoC for the rootkit?	C. Pop-ups demanding a ransom (Ch. 3, Q2)
Nathan works at a school and notices one of his staff appears to have logged in and changed grades for a single student to higher grades for a single student to higher grades, even in classes the staff member is not responsible for. When asked, the staff member says that they did not perform the action. Which of the following is the most likely way that a student could have gotten access to the staff member's password?	A. A keylogger
Amanda notices traffic between her systems and a known malicious host on TCP port 6667. What type of traffic is she most likely detecting? A. Command and control B. A hijacked web browser C. A RAT D. A worm	A. Command and control
Mike discovers that attackers have left software that allows them to have remote access to systems on a computer in his company's network. How should he describe or classify this malware? A. A worm B. Crypto malware C. A Trojan D. A backdoor	D. A backdoor
What is the primary impact of bloatware?	A. Consuming resources
What type of malware is used to gather information about a user's browsing habits and system?	C. Spyware

Matt uploads a malware sample to a third-party malware scanning site that uses multiple antimalware and antivirus engines to scan the sample. He receives several different answers for what the malware package is. What has occurred?	D. Different vendors use different names for malware packages
Nancy is concerned that there is a software keylogger on the system she is investigating. What data may have been stolen?	D. Keyboard and other input from the user
A system in Elaine's company has suddenly displayed a message demanding payment in Bitcoin and claiming that the data has been encrypted. What type of malware has Elaine likely encountered?	C. Ransomware
Rick believes that a system he is responsible for has been compromised with malware that uses a rootkit to obtain and retain access to the system. When he runs a virus scan, the system doesn't show any malware. If he has other data that indicates the system is infected, what should his next step be if he wants to determine what malware may be on the system?	B. Mount the drive on another system and scan it that way
A recently terminated developer from Jaya's organization has contacted the organization claiming that they left code in an application that they wrote that will delete files and bring the application down if they are not employed by the company. What type of malware is this?	C. A logic bomb
Selah wants to ensure that malware is completely removed from a system. What should he do in order to ensure this?	B. Wipe the drive and reinstall from known good media
What is the difference between a worm and a virus?	B. How they spread
Ben wants to analyze Python code that he believes may be malicious code written by an employee of his organization. What can he do to determine if the code is malicious? A. Run a decompiler against it to allow him to read the code. B. Open the file using a text editor to review the code. C. Test the code using an antivirus tool. D. Submit the Python code to a malware testing website.	B. Open the file using a text editor to review the code
Which of the following defenses is most likely to prevent Trojan installation?	B. Preventing downloads from application stores
Jason's security team reports that a recent WordPress vulnerability seems to have been exploited by malware and that their organization's entire WordPress service cluster has been infected. What type of malware is most likely involved if a vulnerability in the software was exploited over the network?	C. A worm
Hui's organization recently purchased new Windows computers from an office supply store. The systems have a number of unwanted programs on them that load at startup that were installed by the manufacturer. What type of software is this?	D. Bloatware
What type of malware connects to a command and control system, allowing attackers to manage, control and update it remotely?	A. A bot
Randy believes that a system that he is responsible for was infected after a user picked up a USB drive and plugged it in. The user claims that they only opened one file on the drive to see who might own it. What type of malware is most likely involved?	A. A virus
Joesph receives an email notifying him that needs to change his password due to a recent account issue. He notices that the email links him to a website using the domain amaz@n.com. What type of atttack should he describe this as?	B. Phishing
When you combine phishing with VoIP, it is known as? A. Spoofing B. Spooning	D. Vishing

C. Whaling D. Vishing	
While reviewing her logs, Michele notices that a remote system has attempted to log into her server via SSH using the username admin and a variety of passwords including "password" and "ninja." What type of attack has Michele noticed?	A. A brute-force attack
Joanna wants to detect password spraying attacks. What type of rule should she deploy through her security systems?	C. Match repeated use of the same password during failed login attempts for multiple usernames
One of the staff at Susan's organization has reported that a critical vendor has contacted them about an unpaid invoice. After Susan investigates, she discovers that the invoice was sent from an email account that was not typically a contact and that the invoice requested payment to a PayPal account. What type of social engineering attack has Susan most likely discovered?	B. Business email compromise
Selah infects the ads on a website that users from her target company frequently visit with malware as part of her penetration test. What technique has she used? A. A watering hole attack B. Vishing C. Whaling D. Typosquatting	A. A watering hole attack
Ben wants to determine if brute-force password attacks are being used against his company. What log information is least likely to be useful when working to detect brute-force attacks?	D. The geographic location of the system being logged into
Melissa receives a call and the caller informs her a senior manager in her organization needs her to buy gift cards for an event that starts in an hour. The caller says that the senior leader forgot to get the cards, and that the event is critical to the organization. Melissa buys the cards and then sends them to the Gmail address the caller says that the senior leader needs them sent to. What type of attack has Melissa fallen for?	B. Pretexting (Ch. 4, Q7)
Alaina wants to determine if a password spraying attack was used against her organization. Which of the following indicators would be most useful as part of her investigation?	B. The passwords used for the failed attempts
Which of the following human vectors is primarily associated with nation-state actors?	A. Misinformation campaigns
Nicole accidentally types www.smazon.com into her browser and discovers that she is directed to a different site loaded with ads and pop-ups. Which of the following is the most accurate description of the attack she has experienced? A. DNS hijacking B. Pharming C. Typosquatting D. Hosts file compromise	C. Typosquatting
Devon is a penetration tester and sets up malicious tools on his target organization's primary website. What type of attack is he conducting?	B. A watering hole attack
Phishing emails sent pretending to be from a company that recipients are familiar with and likely to respond to is what type of attack?	C. Brand impersonation
When a caller was recently directed to Amanda, who is a junior IT employee at her company, the caller informed her that they were the head of IT for her organization and that she needed to immediately disable the organization's firewall due to an ongoing issue with their e-commerce website. After Amanda made the change, she discovered that the caller was not the head of IT, and that	

it was actually a penetration tester hired by her company. Which social engineering principle best matches this type of attack? A. Authority B. Consensus C. Scarcity D. Trust	Impersonation
Fred is concerned aout text message-based attacks. Which of the following attacks relies on text messages as its primary focus?	C. Smishing
Sharif notices his authentication logs have many different user-names showing failed logins with the same password. What type of attack has he discovered?	D. Spraying
Naomi receives a report of smishing. What type of attack should she be looking for? A. Compressed files in phishing B. Text message-based phishing C. Voicemail-based phishing D. Server-based phishing	B. Text message-based phishing
Jack's organization wants to prevent typosquatting. What option should he select to address this issue?	B. Purchase the most common typos for his organization's domain
Gwyne's company has been contracted by customers asking about a new social media account operating under the company's brand. The social media account is advertising cryptocurrency, which Gwyne's organization does not sell or work with. What type of attack best describes what Gwyne's organization has encountered?	B. Brand impersonation
Nation-state-driven social media campaigns about the trustworthiness of the U.S. election in 2016 are what type of social engineering?	C. Disinformation
Which of the following security assessment techniques assumes that an organization has already been compromised and searches for evidence of that compromise?	C. Threat hunting
Renee is configuring her vulnerability management solution to perform credentialed scans of servers on her network. What type of account should she provide to the scanner?	D. Read-only
Ryan is planning to conduct a vulnerability scan of a business-critical system using dangerous plug-ins. What would be the best approach for the initial scan?	C. Run the scan in a test environment
Which of the following values for the CVSS attack complexity metric would indicate that the specified attack is simplest to exploit?	C. Low
Tara recently analyzed the results of a vulnerability scan report and found that a vulnerability reported by the scanner did not exist because the system was actually patched as specified. What type of error occurred?	A. False positive
Brian ran a penetration test against a school's grading system and discovered a flaw that would allow students to alter their grades by exploiting a SQL injection vulnerability. What type of control should he recommend to the school's cybersecurity team to prevent students from engaging in this type of activity? A. Confidentiality B. Integrity C. Alteration D. Availability	B. Integrity
Which of the following security assessment tools is least likely to be used during the reconaissance phase of a penetration test?	C. Metasploit
Which of the following tools is most likely to detect an XSS vulnerability?	B. Web application vulnerability scanner

During a penetration test, Patrick deploys a toolkit on a compromised system and uses it to gain access to other systems on the same network. Which term best describes this activity?	A. Lateral movement
Zian is a cybersecurity leader who is coordinating the activities of a security audit. The audit is being done to validate the organization's financial statements to investors and involves a review of cybersecurity controls. What term best describes this audit?	A. External audit
Which of the following assessment techniques is designed to solicit participation from external security experts and reward them for discovering vulnerabilities?	C. Bug bounty
Kyle is conducting a penetration test. After gaining access to an organization's database server, he installs a backdoor on the server to grant himself access in the future. What term best describes this action? A. Privilege escalation B. Lateral movement C. Maneuver D. Persistence	D. Persistence
Which one of the following techniques would be considered passive reconaissance?	C. WHOIS lookups
Which element of the SCAP framework can be used to consistently describe vulnerabilities?	B. CVE (Common Vulnerabilities and Exposures)
Bruce is conducting a penetration test for a client. The client provided him with the full details of their systems in advance. What type of test is Bruce considering?	C. Known environment test
Lila is working on a penetration testing team and she is unsure whether she is allowed to conduct social engineering as part of the test. What document should she consult to find this information? A. Contract B. Statement of work C. Rules of engagement D. Lessons learned report	C. Rules of engagement
Grace would like to determine the operating system running on a system that she is targeting in a penetration test. Which one of the following techniques will most likely provider her with this information?	B. Footprinting
Kevin recently identified a new security vulnerability and computed its CVSS base score as 6.5. Which risk category would this vulnerability fall into? A. Low B. Medium C. High D. Critical	B. Medium
Which one of the CVSS metrics would contain information about the number of times that an attacker must successfully authenticate to execute an attack?	C. PR
Understanding CVSS	CVSS 3.0:Attack Vector (P/L/A/N):Attack Complexity(H/L):Privileges Required(H/L/N):User Interaction(N/R):Confidentiality(N/L/H):Integrity(N/L/H):Availability(N/L/H):Scope(U/C)
Adam is conducting software testing by reviewing the source code of the application. What type of cost testing is Adam conducting?	B. Static code analysis
Charles is worried about users conducting SQL injection attacks. Which of the following solutions will best address his concerns?	C. Performing user input validation
Precompiled SQL statements that only require variables to be input are an example of what type of application security control?	A. Parameterized queries

During a web application test, Ben discovers that the application shows SQL code as part of an error provided to application users. What should he note in his report? A. Improper error handling B. Code exposure C. SQL injection D. A default configuration issue	A. Improper error handling
The application that Scott is writing has a flaw that occurs when two operations are running at the same time, resulting in unexpected results when the two actions do not occur in the expected order. What type of flaw does this application have?	B. A race condition
Every time Susan checks code into her organization's code repository, it is tested and validated, and then if accepted, it is immediately put into production. What is the term for this?	B. Continuous delivery
Tim is working on a change to a web application used by his organization to fix a known bug. What environment should he be working in?	B. Development
Ricky is concerned that developers in his organization make use of third-party code in their applications, which may introduce unknown vulnerabilities. He is concerned about the risk of the organization running code that it is not aware it is using. Which of the following activities would best address this risk?	B. Package monitoring
Which of the following is not an advantage of automation in cybersecurity operations?	B. Technical debt
Chris is creating a script that will automatically screen any user requests and flag those that exceed normal thresholds for manual review. What term best describes this automation use case?	B. Guard rails
Which one of the following is not a common drawback of automating cybersecurity operations?	A. Reducing employee satisfaction
Frank is investigating a security incident where the attacker entered a very long string into an input field, which was followed by a system command. What type of attack likely took place? A. Cross-site request forgery B. Server-side request forgery C. Command injection D. Buffer overflow	D. Buffer overflow
What type of attack places an attacker in the position to eavesdrop on communications between a user and a web server?	A. On-path attack
Tom is a software developer who creates code for sale to the public. He would like to assure his users that the code they receive actually came from him. What technique can he use to best provide this assurance?	A. Code signing
Chris is reviewing evidence of a cross-scripting attack where the where the attacker embedded JavaScript in a URL that a user clicked. The web page then sent the JavaScript to the user in the displayed page. What term best describes this attack?	A. Reflected XSS
www.mycompany.com/servicestatus.php?serviceID=892'%20;DROP%20TABLE%20Services;--	Parameter pollution
www.mycompany.com/servicestatus.php?serviceID=1 www.mycompany.com/servicestatus.php?serviceID=2 www.mycompany.com/servicestatus.php?serviceID=3	The attacker was trying to exploit insecure direct object reference when sending a series of thousands of requests to the same URL coming from a single IP address
Wendy is a penetration tester who wishes to engage in a session hijacking attack. What information is crucial for Wendy to obtain if her attack will be successful? A. Session ticket B. Session cookie	B. Session cookie

C. Username D. User password	
Joe is examining the logs for his web server and discovers that a user sent input to a web application that contained the string WAITFOR. What type of attack was the user likely attempting?	A. Timing-based SQL injection
Mike is sending David an encrypted message using a symmetric encryption algorithm. What key should he use to encrypt the message?	Shared secret key
Shala recently discovered an attack where the attacker managed to force a network user to use weak encryption and then was able to decrypt that content. What term best describes this attack?	A. Downgrade
Norm is using full-disk encryption technology to protect the contents of laptops against theft. What goal of cryptography is he attempting to achieve?	D. Confidentiality
Brian discovers that a user suspected of stealing sensitive information is posting many image files to a message board. What technique might the individual be using to hide sensitive information in those images?	A. Steganography
Which of the following statements about cryptographic keys is incorrect?	A. All cryptographic keys should be kept secret
What type of cipher operates on one character of text at a time?	C. Stream cipher
Vince is choosing a symmetric encryption algorithm for use in his organization. He would like to choose the strongest algorithm from the choices below. What algorithm should he choose?	D. AES
Kevin is configuring a web server to use digital certificates. What technology can he use to allow clients to quickly verify the status of that digital certificate without contacting a remote server?	B. OCSP
Acme Widgets has 10 employees and they all need the ability to communicate with one another using a symmetric encryption system. The system should allow any two employees to securely communicate without other employees eavesdropping. If an 11th employee is added to the organization, how many new keys must be added to the system?	10 (= one per employee)
Referring to the scenario in question 144, if Acme Widgets switched to an asymmetric encryption algorithm, how many keys would be required to add the 11th employee?	Two keys
What type of digital certificate provides the greatest level of assurance that the certificate owner is who they claim to be?	EV (Extended Validation)
Glenn recently obtained a wildcard certificate for *. mydomain.com. Which one of the following domains would not be covered by this certificate?	dev.www.mydomain.com
Which one of the following servers is almost always an offline CA in a large PKI deployment?	A. Root CA
Which of the following certificate formats is closely associated with Windows binary certificate files?	C. PFX
What type of security solution provides a hardware platform for the storage and management of encryption keys?	A. HSM
What type of cryptographic attack attempts to force a user to reduce the level of encryption that they use to communicate with a remote server?	C. Downgrade
David would like to send Mike a message using an asymmetric encryption algorithm. What key should he use to encrypt the message?	C. Mike's public key

WHEN MIKE RECEIVES THE MESSAGE THAT DAVID ENCRYPTED FOR HIM, WHAT KEY SHOULD HE USE TO DECRYPT THE MESSAGE? A. DAVID'S PUBLIC KEY B. DAVID'S PRIVATE KEY C. MIKE'S PUBLIC KEY D. MIKE'S PRIVATE KEY	D. Mike's private key
If David wishes to digitally sign the message that he is sending Mike, what key would he use to create the digital signature?	B. David's private key
When Mike receives the digitally signed message from David, what key should he use to verify the digital signature?	A. David's public key
Angela has chosen to federate with other organizations to allow use of services that each organization provides. What role does Angela's organization play when they authenticate their users and assert that those users are valid to other members of the federation?	D. Identity provider
Which of the following technologies is the least effective means of preventing shared accounts?	A. Password complexity requirements
What major difference is likely to exist between on-premises identity services and those used in a cloud-hosted environment?	B. The cloud service will provide account and identity management services
Amitoj wants to ensure that her organization's password policy does not allow users to reset their password multiple times until they can reuse their current password. What setting is used to prevent this?	D. Age
Which type of multifactor authentication is considered the least secure?	B. SMS
Geeta has been issued a USB security key as part of her organization's multifactor implementation. What type of implementation is this?	A. A hard token
Michelle enables the Windows picture password feature to control logins for her laptop. Which type of attribute will it provide?	B. Something you know
What purpose would Linux file permissions set to rw-r-r-- serve?	To allow the owner to read and write the file, and for the owner's group and others to be able to read it.
Theresa wants to implement an access control scheme that sets permissions based on what the individual's job requires. Which of the following schemes is most suited to this type of implementation?	C. RBAC
Which of the following biometric technologies is most broadly deployed due to its ease of use and acceptance from end users?	D. Fingerprint scanner
Adam wants to increase his organization's passwords resistance to attacks in the event that the password hash database is stolen by attackers. Which of the following password security settings has the largest impact on password cracking if his organization's current passwords are 8 characters long?	B. Password length
A PIN is an example of what type of factor?	Something you know
Marie is implementing a PAM solution and wants to ensure that root passwords are available in the event of an outage. Which PAM-related tool is most likely to be useful in the situation?	C. Password vaulting
Jill sets her files on a Windows file share to allow Fred access to the files. What type of access control system is she using?	D. Discretionary access control
Lisa sets up an account on a website that allows her to log in with Google. When she logs in, Google provides an access token to the website that confirms that she is who she says she is but	OAuth

doesn't provide the site with her password. Which of the following technologies has she used?	
Kyle has been asked to provide his government-issued ID as part of the creation of his user account. What process should he assume it is being used for?	C. Identity proofing
What key concept below best describes only providing the permissions needed to form a role?	A. Least privilege
Nina has recently left her organization. What should the organization do with her account?	C. Deprovision her account
A person's name, age, location or job title are all examples of what?	C. Attributes
What type of access control scheme best describes the Linux filesystem?	C. Discretionary Access Control (DAC)
Naomi wants to handle increasing load by scaling cloud-based resources as needed while having the change remain transparent to users. She also wants to allow for upgrades and system replacements transparently. What solution should she select?	A. Load balancing
Rick performs a backup that captures the changes since the last full backup. What type of backup has he performed?	D. A differential backup
What type of recovery site has some or most systems in place but does not have the data needed to take over operations?	B. A warm site
Ben wants to test his warm site to verify that it will take over operations successfully. What type of testing is this?	Failover
Felix wants to clone a virtual machine. What should he do to capture a live machine, including the machine state?	B. A snapshot
Sally is working to restore her organization's operations after a disaster took her datacenter offline. What critical document should she refer to as she restarts systems?	A. The restoration order documentation
Mike wants to stop vehicles from traveling toward the entrance of his building. What physical security control should he implement?	A bollard
Alecia wants to ensure that her backups cannot be accessed by third parties while stored in an offsite storage location. What should she do to secure her backups?	D. Encrypt the backup data
Fred wants to be able to recover his DB transactions at any point in time if a physical disaster occurs involving his datacenter. His organization uses daily backups. What additional solution should he select to support this need?	C. Offsite journaling
Ellen is concerned about her company's resilience and wants to ensure that it can handle either changing loads or support disaster recovery and business continuity efforts if a primary location or datacenter were taken offline. Which of the following should she primarily focus on during her capacity planning?	People, technology, infrastructure
Madhuri has deployed a replication tool that copies data over to a secondary hot site in real time. What type of replication has she deployed?	A. Synchronous replication
What factor is a major reason organizations do not use security guards?	C. Cost
Megan wants to deploy a sensor that is inexpensive, yet will allow her to detect humans entering and moving in a secured room. Which of the following should she select?	A. An infrared sensor
Kathleen wants to discourage potential attackers from entering the facility she is responsible for. Which of the following is not a common control used for this type of preventive defense?	C. Platform diversity

How does technology diversity ensure cybersecurity resilience?	1) It ensures that a vulnerability in a single company's product will not impact the entire infrastructure, 2) If a single vendor goes out of business, the company does not need to replace its entire infrastructure, 3) It means a misconfiguration will not impact the company's entire infrastructure
Scott sends his backups to a company that keeps them in a secure vault. What type of backup solution has he implemented? A. Nearline B. Safe C. Online D. Offline	D. Offsite
Gabby wants to detect brute-force attempts against her organization. What solution is best suited to this?	A. Security guards
Florian wants to test his HA designs but does not want to interrupt his organization's normal work. Which of the following is the least disruptive testing scenario?	B. A tabletop exercise
Access control vestibule	Access control vestibules, also known as security or mantrap vestibules, are a highly effective means of hardening commercial security. These enclosed entryways are designed to restrict and monitor access to a building by allowing only one person to enter at a time, typically through a series of interlocking doors
Gurvinder identifies a third-party datacenter provider over 90 miles away to run his redundant datacenter operations. Why has he placed the datacenter that far away?	C. Geographic dispersion
Kevin discovered that his web server was being overwhelmed by traffic, causing a CPU bottleneck. Using the interface offered by his cloud service provider, he added another CPU to the server. What term best describes Kevin's action?	C. Vertical scaling
Fran's organization uses a Type I hypervisor to implement an IaaS offering that it sells to customers. Which of the following security controls is least applicable to this environment?	C. The provider must maintain security patches on the host operating system
In what cloud security model does the cloud service provider bear the most responsibility for implementing security controls?	D. SaaS
Greg would like to find a reference document that describes how to map cloud security controls to different regulatory standards. What document would best assist with this task?	A. CSA CCM
Wanda is responsible for a series of seismic sensors placed at remote locations. These sensors have low-bandwidth connections and she would like to place computing power on the sensors to allow them to preprocess data before it is sent back to the cloud. What term best describes this approach?	A. Edge computing
Which one of the following statements about cloud computing is incorrect?	C. Cloud computing customers provision resources through the service provider's sales team
Helen designed a new payroll system that she offers to her customers. She hosts the payroll system in AWS and her customers access it through the web. What tier of cloud computing best describes Helen's service?	B. SaaS
Which cloud computing deployment model requires the use of a unifying technology platform to tie together components from different providers?	D. Hybrid cloud
Which of the following would not commonly be available as an IaaS service offering?	A. CRM
Which one of the following is not an example of infrastructure as code?	C. Using a cloud provider's web interface to provision resources

Brian is selecting a CASB for his organization and he would like to use an approach that interacts with the cloud provider directly. Which CASB approach is most appropriate for his needs? A. Inline CASB B. Outsider CASB C. Comprehensive CASB D. API-based CASB	D. API-based CASB
In which of the following cloud categories are customers typically charged based on the number of virtual server instances dedicated to their use?	C. IaaS and PaaS
Brian would like to limit the ability of users inside his organization to provision expensive cloud server instances without permission. What type of control would best help him achieve his goal?	A. Resource policy
Ursula would like to link the networks in her on-premises datacenter with cloud VPCs in a secure manner. What technology would help her best achieve her goal?	A. Transit gateway
What component of a virtualization platform is primarily responsible for preventing VM escape attacks?	D. Hypervisor
Ryan is selecting a new security control to meet his organization's objectives. He would like to use it in their multicloud environment and would like to minimize the administrative work required from his fellow technologists. What approach would best meet his needs?	A. Third-party control
Kira would like to implement a security control that can implement access restrictions across all of the SaaS solutions used by her organization. What control would best meet her needs?	C. CASB
Howard is assessing the legal risks to his organization based on its handling of PII. The organization is based in the United States, handles the data of customers located in Europe, and stores information in Japanese datacenters. What law would be most important to Howard during his assessment?	D. All should have equal weight
Brenda's company provides a managed incident response service to its customers. What term best describes this type of service offering?	D. MSSP
Tony purchases virtual machines from Microsoft Azure and uses them exclusively for use by his organization. What model of cloud computing is this?	A. Public cloud
Lin's hardware manufacturer has stopped selling the model of device that Lin's organization uses and has also stopped providing security or other updates. What phase of the hardware lifecycle is the device in?	B. Legacy
Naomi has discovered the following TCP ports open on a system she wants to harden. Which ports are used for unsecure services and thus should be disabled to allow their secure equivalents to continue to be used? 21 22 23 80 443 A. 21, 22, and 80 B. 21 and 80 C. 21, 23, and 80 D. 22 and 443	C. 21, 23 and 80
Frank's organization is preparing to deploy a data loss prevention (DLP) system. What key process should they undertake before they deploy it?	C. Implement and use a data classification scheme

Oliver wants to store and manage secrets in his cloud service provider's environment. What type of solution should he look for as part of their offerings?	C. A KMS
What is the key difference between EDR and XDR solutions?	C. The breadth of the technology stack that is covered
Michelle wants to prevent unauthorized applications from being installed on a Windows system. What type of tool can she use to stop applications from being used?	B. A GPO
What term is used to describe tools focused on detecting and responding to suspicious activites occurring on endpoints like desktops, laptops and mobile devices?	A. EDR
Fred has recently purchased a network router and is preparing to deploy it. Which of the following is a common step in deploying new routers?	D. Changing default passwords
Charlene wants to prevent attacks against her system that leverage flaws in the services that it provides while still keeping the services accessible. What hardening technique should she use?	B. A host-based IPS
Allan is preparing to harden his organization's network switches. Which of the following is not a common hardening technique for network devices?	A. Removing unnecessary software
Helen's organization is planning to deploy IoT devices across their buildings as part of a HVAC system. Helen knows that the vendor for IoT devices does not provide regular security updates to the device's web interfaces that are used to manage the devices. What security control should she recommend to help protect the devices on the network?	B. Deploy the IoT devices to a protected VLAN
What is the primary reason to remove unnecessary software during hardening efforts?	A. To reduce the attack footprint of the device
Brian has deployed a system that monitors sensors and uses that data to manage the power distribution for the power company that he works for. Which of the following terms is commonly used to describe this type of control and monitoring solution?	A. SCADA
The organization that Lynn works for wants to deploy an embedded system that needs to process data as it comes to the device without processing delays or other interruptions. What type of solution does Lynn's company need to deploy?	D. An RTOS
Which of the following is not a common constraint of an embedded system?	B. Cost
Jim configures a Windows machine with the built-in BitLocker full disk encryption tool. When is the machine least vulnerable to having data stolen from it? A. When the machine is off B. When the machine is booted and logged in but is locked C. When the machine is booted and logged in but is unlocked D. When the machine is booted and logged in but is asleep	A. When the machine is off
Olivia wants to install a host-based security package that can detect attacks against the system coming from the network, but she does not want to take the risk of blocking the attacks since she fears that she might inadvertently block legitimate traffic. What type of tool could she install that will meet this requirement?	B. A host-based intrusion detection system
Anita wants to enforce security settings across her organization's Windows Active Directory domain. What tool can she use to do this?	B. Group Policy
Chris want systems that connect to his network to report their boot processes to a server where they can be validated before being permitted to join the network. What technology should he use to do this on the workstations?	UEFI/measured boot

Elaine wants to securely erase the contents of a tape used for backups in her organization's tape library. What is the fastest secure erase method available to her that will allow the tape to be reused?	A. Using a degausser
A system that Tony manages sends an SNMP trap. What type of information should Tony expect to receive?	C. Notification of an issue
Ben wants to observe malicious behavior targeted at multiple systems on a network. He sets up a variety of systems and instruments to allow him to capture copies of attack tools and to document all the attacks that are conducted. What has he set up?	C. A honeypot
Valerie wants to replace the telnet access that she found still in use in her organization. Which protocol should she use to replace it, and what port will it run on?	SSH, port 22
Jill wants to use DNS filtering to prevent users in her organization from visiting potentially malicious sites. What type of service should she use to obtain this information?	D. A reputation service
Chuck wants to provide access to a protected network from a less trusted network. What type of solution is commonly implemented to provide a secure, monitored access network?	B. A jump server
Kathleen wants to deploy a firewall that can handle large amounts of network traffic while performing advanced firewalling tasks. What type of device should she select?	A. A NGFW
Mark wants to prevent DNS poisoning attacks. What technology should she select to help manage this?	C. SD-WAN
What protocol is used to securely wrap many otherwise insecure protocols?	D. TLS
Valentine wants to deploy a secure version of DHCP for her organization. What should she implement?	D. There is no secured version of DHCP
What component of a zero-trust architecture forwards requests from subjects and acts on whether subjects are allowed to access resources?	B. Policy enforcement points
Gary wants to use secure protocols for email access for his end users. Which of the following groups of protocols should he implement to accomplish this task?	C. POPS, IMAPS, HTTPS
Gary wants to prevent his organization's most sensitive data from being accessed by network-based attackers at any cost. What solution should he implement to ensure this?	A. An air gap
Madhuri is designing a load-balancing configuration for her company and wants to keep a single node from being overloaded. What type of design will meet this need? A. A daisy chain B. Active/active C. Duck-duck-goose D. Active/passive	B. Active/active
What type of NAC will provide Isaac with the greatest amount of information about the systems that are connecting while also giving him the most amount of control of systems and their potential impact on other systems that are connected to the network? A. Agent-based, pre-admission NAC B. Agentless, post-admission NAC C. Agent-based NAC, post-admission NAC D. Agent-based, post-admission NAC	A. Agent-based, pre-admission NAC
Danielle's organization has implemented a tool that combines SD-WAN, a CASB, and Zero Trust, among other security functions, among other security functions, to provide security regard-	D. SASE

less of where her organization's devices are. What type of solution has her organization implemented?	
Wayne is concerned that an on-path attack has been used against computers he is responsible for. What artifact is he most likely to find associated with this attack?	B. A browser plug-in
Elle has scanned her organization from an external IP address and has identified all of the devices that are visible from the public Internet. What does this enable her to describe?	C. Her organization's attack surface
What technique is used to ensure that DNSSEC-protected DNS information is trustworthy?	A. It is digitally signed
Fred wants to ensure that the administrative interfaces for the switches and routers are protected so that they cannot be accessed by attackers. Which of the following solutions should he recommend as part of his organization's network design?	C. Out of band management
Alyssa wants to harden iOS devices her organization uses. What set of guidelines can she follow to align to common industry practices?	B. CIS benchmarks
FRED'S COMPANY ISSUES DEVICES IN A BYOD MODEL. THAT MEANS THAT FRED WANTS TO ENSURE THAT CORPORATE DATA AND APPLICATIONS ARE KEPT SEPARATE FROM PERSONAL APPLICATIONS ON THE DEVICES. WHAT TECHNOLOGY IS BEST SUITED TO MEET THIS NEED? A. BIOMETRICS B. FULL-DEVICE ENCRYPTION C. CONTEXT-AWARE AUTHENTICATION D. CONTAINERIZATION	D. Containerization
Michelle has deployed iPads to her staff who work her company's factory floor. She wants to ensure that the devices work only in the factory and that if they are taken home they cannot access business data or services. What type of solution is best suited to her needs? A. Context-aware authentication B. Geofencing C. Geolocation D. Unified endpoint management (UEM)	B. Geofencing
Ivan is running an enterprise wireless network and his heatmap shows that two access points are likely conflicting with each other. What will the enterprise access controller most likely do to handle this conflict?	D. Decrease the broadcast power of the access points.
Chris wants to use geolocation technology to find where phones issued by his organization are located. Which of the following is not commonly used as part of geolocation techniques?	C. NFC
Daniel knows that WPA3 has added a method to ensure that brute-force attacks against weak preshared keys are less likely to succeed. What is this technology called?	A. SAE
Isabelle needs to select the EAP protocol that she will use with her wireless network. She wants to use a secure protocol that does not require client devices to have a certificate, but she does want to require mutual authentication. Which EAP protocol should she use?	C. PEAP
Theresa has implemented a technology that keeps data for personal use separate from data for her company on mobile devices used by members of her staff. What is this concept called?	A. Storage segmentation
A member of Jake's organization tells him that he sideloaded applications on his Android-based company owned phone. What has occurred?	C. Applications were installed by copying them instead of via an app store

Madhuri disables SMS, MMS, and RCS on phones in her organization. What has she prevented from being sent? A. Phone calls and texts B. Text messages and multimedia messages C. Text messages and firmware updates D. Phone calls and multimedia messages	B. Text messages and multimedia messages
What is the most frequent concern that leads to GPS tagging being disabled by some companies via an MDM tool?	C. Privacy
Bart wants to use a cellular hotspot to provide Internet connectivity via Wi-Fi. What type of network has he set up for his laptop and phone to connect to?	A. Ad-hoc
Susan wants to ensure that the threat of a lost phone creating a data breach is minimalized. What two technologies should she implement to do this?	A. Wi-fi and NFC
What are the two most commonly deployed biometric authentication solutions for mobile devices?	C. Face recognition and fingerprint recognition
Alaina wants to modify operating system settings and features on her iOS device and to install applications that are not permitted or available via the Apple App Store. What would she need to do to accomplish this?	B. Jailbreak the phone
Jerome wants to allow guests to use his organization's wireless network, but he does not want to provide a preshared key. What solution can he deploy to gather information such as email addresses or other contact information before allowing users to access his open network?	D. A captive portal
Amanda wnats to create a view of buildings that show Wi-Fi signal strength and coverage. What is this type of view called?	C. A heatmap
Megan wants to prevent access to phones that are misplaced by members of her organization. Which of the following MDM control options is least likely to help her protect phones that are misplaced?	D. Application management
Gurvinder wants to select a mobile device deployment method that provides employees with devices that they can use as though they're personally owned to maximize flexibility and ease of use. What deployment model should he select?	A. CYOD
Octavia discovers that the contact list from her phone has been acquired via a wireless attack. Which of the following is the most likely culprit?	C. Bluesnarfing
What is the Security+ incident response cycle?	Monitoring, Detection, Analysis, Containment, Eradication, Recovery
Michael analyzes network traffic, including packet content, as part of his incident response process. What tool should he use?	C. Packet capture
Susan wants to create a dashboard that shows her aggregated log events related to logins from different geographic regions. Her goal is to identify impossible travel scenarios. Which of the following solutions should she select to accomplish that goal?	C. SIEM
Selah wants to ensure that users in her organization can only install applications that are evaluated and approved by the organization's security team. What should she use?	C. An application allow list
What is the primary concern with sFlow in a large, busy network? (1)	sFlow samples only network traffic, meaning that some detail will be lost
Mark unplugs the network connection from a system that is part of an incident and places tape over its Ethernet jack with a sign that says "Do not reconnect without approval from IR team." How is this method best described? (1) A. Containment	B. Isolation

B. Isolation C. Segmentation D. Zoning	
What is the primary concern with sFlow in a large, busy network? (1)	D. sFlow samples only network traffic, meaning that some detail will be lost
The company that Ben works for wants to test its incident response plan. Ben gathers the incident response team in a room and walks through a scenario to validate the organization's policies and procedures. What type of event has Ben hosted?	C. A tabletop exercise
Madhuri wants to check a PNG-formatted photo for GPS coordinates. Where can she find that information if it exists in the photo?	C. In the photo's metadata
Alyssa has identified malware on a system. She removes the system from the network to ensure that it cannot impact other systems. What technique has she used to deal with this system?	A. Quarantine
Kristen discovers missing logs as part of her threat hunting activities. What has most likely happened?	C. An attacker wiped logs to hide evidence
Ian has been receiving hundreds of false positive alerts from his SIEM every night when scheduled jobs run across his datacenter. What should he adjust on his SIEM to reduce the false positive rate? A. Trend analysis B. Sensitivity C. Correlation rules D. Dashboard configuration	B. Sensitivity
Which team member acts as a primary conduit to senior management on an IR team?	C. Management
Dana is reviewing her system's application logs and notices that a full backup of the application was done at 10am. She knows that the job that runs the backup process is set to run overnight. What indicator should she flag this as?	Out of cycle logging
Jim wants to view log entries that describe actions taken by applications on a Red Hat Linux system. Which of the following tools can he use on the system to view those logs?	C. journalctl
Megan wants to ensure that logging is properly configured for her organization's Windows workstations. What could she use to ensure that logging best practices are configured?	B. Benchmarks
Chris has turned on logon auditing for a Windows system. Which log will show them?	B. The Windows Security log
Jayne wants to determine why a ransomware attack was successful against her organization. She plans to conduct a root cause analysis. Which of the following is not a typical root cause analysis method?	A. Root/branch review
Hitesh wants to keep a system online but limit the impact of the malware that was found on it while an investigation occurs. What method from the following list should he use?	A. Containment
What phase in the incident response process leverages indicators of compromise and log analysis as part of a review of events?	D. Identification
Henry wants to check to see if services were installed by an attacker. What commonly gathered organizational data can he use to see if a new service appeared on systems? A. Registry dumps from systems throughout his organization B. Firewall logs C. Vulnerability scans D. Flow logs	C. Vulnerability scans
	C. dd

Felix wants to make an exact copy of a drive using a Linux command line tool as part of a forensic acquisition process. What command should he use?	
Greg is preparing a forensic report and needs to describe the tools that were used. What should he report about the tools in addition to their name?	C. Any known limitations or issues with the tools
Gabby is preparing chain of custody documentation and identifies a gap in hand off documentation for an original source forensic drive. What issue should she expect to encounter due to this gap?	A. The evidence may not be admissible in court
Mike's organization has recently moved to a SaaS cloud service and needs to collect forensic data from the cloud service. What process can Mike use to gather the information he needs?	B. Identify the log information available and request any other desired information from the cloud service provider
Charles wants to obtain a forensic copy of a running virtual machine. What technique should he use to capture the image?	C. Use the VM host to create a snapshot
Melissa wants to capture network traffic for forensic purposes. What tool should she use to capture it?	B. Wireshark
Frank is concerned about the admissibility of his forensic data. Which of the following is not an element he should be concerned about? A. Whether the forensic source data has remained unaltered B. Whether the practices and procedures would survive review by experts C. Whether the evidence is relevant to the case D. Whether the forensic information includes a timestamp	D. Whether the forensic information includes a time stamp
What is the document that tracks the custody or control of a piece of evidence called?	D. Chain of custody
Isaac is performing a forensic analysis on two systems that were compromised in the same event in the same facility. As he performs his analysis, he notices the event appears to have happened exactly one hour earlier on one system than the other. What is the most likely issue he has encountered?	B. One system is set to an incorrect time zone.
What legal concept determines the law enforcement agency or agencies that will be involved in a case based on location?	C. Jurisdiction
Michael wants to acquire the firmware from a running device for analysis. What method is most likely to succeed?	A. Use forensic memory acquisition techniques
Charles needs to know about actions an individual performed on a PC. What is the best starting point to help him identify those actions?	C. Interview the individual
Maria has acquired a disk image from a hard drive using dd, and she wants to ensure that her process is forensically sound. What should her next step be after completing the copy? A. Securely wipe the source drive. B. Compare the hashes of the source and target drive. C. Securely wipe the target drive. D. Update her chain-of-custody document.	B. Compare the hashes of the source and target drive
Alex has been handed a flash media device that was quick-formatted and has been asked to recover the data. What data will remain on the drive? A. No data will remain on the drive. B. Files will remain but file indexes will not. C. File indexes will remain, but the files will be gone. D. Files and file indexes will remain on the drive.	B. Files will remain but file indexes will not
Naomi is preparing to migrate her organization to a cloud service and wants to ensure that she has the appropriate contractual language in place. Which of the following is not a common item she should include?	B. Right to forensic examination

Alaina wants to maintain chain of custody documentation and has created a form. Which of the following is not a common element on a chain of custody form?	D. Method of transport
Henry is following the EDRM model and is preparing to review data. What two key tasks occur during this stage?	C. Validating that the desired data is included and that information that should not be shared is not included
Theresa's organization has received a legal hold notice for their files and documents. Which of the following is not an action she needs to take?	C. Delete all sensitive documents related to the case
Gurvinder wants to follow the order of volatility to guide his forensic data acquisition. Whcih of the following is the least volatile?	C. Backups
What is the key difference between hashing and checksums?	A. Both can validate integrity, but a hash also provides a unique digital fingerprint
RAID 0 (striping)	Data is spread across all drives in the array. Better I/O performance (speed); all capacity used. Not fault tolerant - all data is lost if a drive is lost
RAID 1 (mirroring)	All data is duplicated to another drive or drives. High read speeds from multiple drives; data available if a drive fails. Uses twice the storage for the same amount of data.
RAID 5 (Striping with parity)	Data is striped across drives, with one drive used for parity (checksum) of the data. Parity is spread across drives as well as data. Data reads reads are fast; data writes are slightly slower. Drive failures can be rebuilt as long as only a single drive fails. Can only tolerate a single drive failure at a time. Rebuilding arrays after a drive loss can be slow and impact performance.
RAID 10 (Mirroring and Striping)	Combines the advantages and disadvantages of both RAID 0 and RAID 1. Sometimes written as RAID 1+0.
If you want to encrypt a message, use the	Recipient's public key
If you want to decrypt a message sent to you, use	Your private key
If you want to digitally sign a message you are sending to someone else, use	Your private key
If you want to verify the signature on a message sent by someone else, use	The sender's public key
Joe is authoring a document that explains to system administrators one way that they might comply with the organization's requirement to encrypt all laptops. What type of document is Joe writing?	B. Guideline
Which one of the following statements is not true about compensating controls under PCI DSS	Controls used to fulfill one PCI DSS requirement may be used to compensate for the absence of a control needed to meet another requirement
What law creates privacy obligations for those who handle the personal information of European Union residents?	C. GDPR
Which of the following is not one of the five core security functions defined by the NIST Cybersecurity Framework?	B. Contain
What ISO standard provides guidance on privacy controls?	ISO 27701
Which one of the following documents must normally be approved by the CEO or similarly high level executive?	D. Policy
Greg would like to create an umbrella agreement that provides the security terms and conditions for all future work that his organization does with a vendor. What type of agreement should Greg use? A. BPA B. MOU	C. MSA

C. MSA D. SLA	
Master Service Agreement (MSA)	provide an umbrella contract for the work that a vendor does with an organization over an extended period of time
Service Level Agreement (SLA)	Are written contracts that specify the conditions of service that will be provided by the vendor and the remedies available to the customer if the vendor fails to meet the SLA. SLAs commonly cover issues such as system availability, data durability and response time.
A memorandum of understanding (MOU)	is a letter written to document aspects of the relationship. MOUs are an informal mechanism that allows the parties to document their relationship to avoid future misunderstandings. MOUs are commonly used in cases where an internal service provider is offering a service to a customer in a different business unit of the company.
A memorandum of agreement (MOA)	is a formal document that outlines the terms and details of an agreement between parties, establishing a mutual understanding of the roles and responsibilities in fulfilling specific objectives. MOAs are generally more detailed than MOUs and may include clauses regrding resource allocation, risk management and performance metrics.
Business partners agreements (BPAs)	exist when two organizations agree to do business with each other in a partnership. For example, if two companies who jointly develop and market a product, the BPA might specify each partner's responsibilities and the division of profits
What organization is known for creating independent security benchmarks covering hardware and software platforms from many different vendors?	B. Center for Internet Security
What do many organizations use to schedule and coordinate changes for information systems?	C. Maintenance windows
Which one of the following would not be normally found in an organization's information security policy?	C. Requirement to use AES256 encryption
Alice, an IT security manager at Acme Corporation, decides to conduct an exercise to test the employees' ability to recognize phishing emails. She creates fake phishing messages and sends them to the employees. When employees click on the links in the fake messages, they are redirected to a training program. What is the primary purpose of the exercise that Alice is conducting?	C. To test employees' ability to recognize phishing messages and help them improve
Tonya discovers that an employee is running a side business from his office, using company technology resources. What policy would most likely contain information relevant to this situation? A. NDA B. AUP C. Data ownership D. Data classification	B. AUP
What compliance obligation applies to merchants and service providers who work with credit card information?	D. PCI DSS
Mike is an information security manager at TechRise Solutions. The company has been experiencing an increase in security incidents, and senior management is concerned about the security posture of the organization. They have asked Mike to take proactive measures to strengthen the company's security culture. What should Mike's primary role in enhancing the security awareness and training at TechRise Solutions?	B. To establish, promote, and maintain security training and awareness programs
Colin would like to implement a security control in his accounting department that is specifically designed to detect cases of fraud	

that are able to occur despite the presence of other security controls. Which one of the following controls is best suited to meet Colin's need? A. Separation of duties B. Least privilege C. Dual control D. Mandatory vacations	D. Mandatory vacations
Which of the following security policy framework components does not contain mandatory guidance for individuals in the organization?	D. Guideline
Rachel is the Head of Security at WebCraft Inc. She wants to create both security training and awareness programs. Which statement best captures the difference between these programs?	A. Security training requires time to learn new material, whereas awareness efforts use techniques like posters and emails to remind employees of security lessons
Allan is developing a document that lists the acceptable use mechanisms for securely obtaining remote administrative access to servers in his organization. What type of document is Allan writing?	B. Standard
Which of the following is not a common use of the NIST Cybersecurity Framework?	D. Create specific technology requirements for an organization
Which one of the following items is not normally included in a request for an exception to security policy?	C. Proposed revision to the security policy
Jen identified a missing patch on a Windows server that might allow an attacker to gain remote control of the system. After consulting with her manager, she applied the patch. From a risk management perspective, what has she done?	C. Removed the vulnerability
You notice a high number of SQL injection attacks against a web application run by your organization, and you install a web application firewall to block many of these attacks before they reach the server. How have you altered the severity of this risk? A. Reduced the magnitude B. Eliminated the vulnerability C. Reduced the probability D. Eliminated the threat	C. Reduced the probability
Aziz is responsible for the administration of an e-commerce website that generates $100,000 per day in revenue for his firm. The website uses a database that contains sensitive information about the firm's customers. He expects that a compromise of that database would result in $500,000 in fines against his firm. Aziz is assessing the risk of a SQL injection attack against the database where the attacker would steal all of the customer personally identifiable information (PII) from the database. After consulting threat intelligence, he believes that there is a 5 percent chance of a successful attack in any given year. What is the asset value (AV)? A. $5,000 B. $100,000 C. $500,000 D. $600,000	C. $500,000
Aziz is responsible for the administration of an e-commerce website that generates $100,000 per day in revenue for his firm. The website uses a database that contains sensitive information about the firm's customers. He expects that a compromise of that database would result in $500,000 in fines against his firm. Aziz is assessing the risk of a SQL injection attack against the database where the attacker would steal all of the customer personally identifiable information (PII) from the database. After consulting threat intelligence, he believes that there is a 5 percent	D. 100%

chance of a successful attack in any given year. What is the exposure factor (EF)?	
Aziz is responsible for the administration of an e-commerce website that generates $100,000 per day in revenue for his firm. The website uses a database that contains sensitive information about the firm's customers. He expects that a compromise of that database would result in $500,000 in fines against his firm. Aziz is assessing the risk of a SQL injection attack against the database where the attacker would steal all of the customer personally identifiable information (PII) from the database. After consulting threat intelligence, he believes that there is a 5 percent chance of a successful attack in any given year. What is the single loss expectancy (SLE)?	C. $500,000
Aziz is responsible for the administration of an e-commerce website that generates $100,000 per day in revenue for his firm. The website uses a database that contains sensitive information about the firm's customers. He expects that a compromise of that database would result in $500,000 in fines against his firm. Aziz is assessing the risk of a SQL injection attack against the database where the attacker would steal all of the customer personally identifiable information (PII) from the database. After consulting threat intelligence, he believes that there is a 5 percent chance of a successful attack in any given year. What is the annualized rate of occurrence (ARO)?	A. 0.05
Aziz is responsible for the administration of an e-commerce website that generates $100,000 per day in revenue for his firm. The website uses a database that contains sensitive information about the firm's customers. He expects that a compromise of that database would result in $500,000 in fines against his firm. Aziz is assessing the risk of a SQL injection attack against the database where the attacker would steal all of the customer personally identifiable information (PII) from the database. After consulting threat intelligence, he believes that there is a 5 percent chance of a successful attack in any given year. What is the annualized loss expectancy (ALE)?	$25,000
Grace recently completed a risk assessment of her organization's exposure to data breaches and that there is a high level of risk related to the loss of sensitive personal information. She is considering a variety of approaches to managing this risk. Grace's first idea is to add a web application firewall to protect her organization against SQL injection attacks. What risk management strategy does this approach adopt?	C. Risk mitigation
Grace recently completed a risk assessment of her organization's exposure to data breaches and that there is a high level of risk related to the loss of sensitive personal information. She is considering a variety of approaches to managing this risk. Business leaders are considering dropping the customer activities that collect and store sensitive personal information. What risk management strategy would this approach use?	B. Risk avoidance
Grace recently completed a risk assessment of her organization's exposure to data breaches and that there is a high level of risk related to the loss of sensitive personal information. She is considering a variety of approaches to managing this risk. Grace's company decided to install the web application firewall and continue doing business. They are still worried about other risks to the information that were not addressed by the firewall	D. Risk transference

and are considering purchasing an insurance policy to cover those risks. What strategy does this use?	
Grace recently completed a risk assessment of her organization's exposure to data breaches and that there is a high level of risk related to the loss of sensitive personal information. She is considering a variety of approaches to managing this risk. In the end, Grace's risk managers found that the insurance policy was too expensive and opted not to purchase it. They are taking no additional action. What risk management strategy is being used in this situation?	A. Risk acceptance
Under the European Union's GDPR, what term is assigned to the individual who leads an organization's privacy efforts?	A. Data protection officer
Helen's organization maintains medical records on behalf of its customers, who are individual physicians. What term best describes the role of Helen's organization?	A. Data processor
Gene recently conducted an assessment and determined that his organization can be without its main transaction database for a maximum of two hours before unacceptable damage occurs to the business. What metric has Gene identified? A. MTBF B. MTTR C. RTO D. RPO	C. RTO
Tina works for a hospital system and manages the system's patient records. What category of personal information best describes the information that is likely to be found in those records? A. PCI B. PHI C. PFI D. PII	B. PHI
Asa believes that her organization is taking data collected from customers for technical support and using it for marketing without their permission. What principle is most likely being violated?	C. Purpose limitation
Which of the following U.S. government classification levels requires the highest degree of security control?	C. Top Secret
Which type of analysis uses numeric data in the analysis, resulting in assessments that allow the very straightforward prioritization of risk?	D. Quantitative
What term is given to an individual or organization who determines the reasons for collecting personal information?	B. Data controller
Brian recently conducted a risk mitigation exercise and has determined the level of risk that remains after implementing a series of controls. What term best describes this risk?	D. Residual risk