Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns? - **Data confidentiality**

These are malicious pieces of computer code and applications that can damage your computer, as well as steal your personal or financial information. - **Software-Based Attacks**

It is the state of being whole and undivided. - **Integrity**

What does confidentiality of data imply to - **Rules which restrict access only to those who need to know**

The process of putting a decision or plan into effect also known as execution. - **Implementation**

PJ is buying books from an online retail location, and she finds that she can alter the cost of a book from $19.99 to $1.99. Which portion of the CIA set of three has been broken? - **Integrity**

What does integrity of data refer to? - **The level of assurance which can be given as to how accurate and trustworthy data is**

What does integrity of information allude to - **The level of assurance which can be given as to how accurate and trustworthy data is**

A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered? - **Steganography**

It is a concept that has employees rotate through different jobs to learn the procedures and processes in each. - **Job rotation**

It is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features - **Authorization**

It is the process of verifying the identity of a person or device. **- Authentication**

It provides two-way authentication - **Multifactor authentication**

During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

SSL 1.0

Which of the following is best practice to put at the end of an ACL?

Implicit deny

It is the assurance that someone cannot deny the validity of something

Non-repudiation

It is an authentication method that identifies and recognizes individuals based on voice recognition or physical characteristics such as a fingerprint, face acknowledgment, iris recognition, and retina check

Biometrics

Electronic records that are not archival. Click here for tips on identifying and deleting electronic records that have met retention.

Delete

It ought to incorporate a well-defined security vision for the organization.

Security policies

A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts. Joe will need network access to all directories, folders and files within the accounting department. Which of the following configurations will meet the requirements?

Create an account with role-based access control for accounting

Paper and electronic records to the University Archives if they have permanent legal, fiscal, administrative, or historical value.

Transfer

It distinguishes the recurrence of overhauling the record definitions as well as how detachable media, mail connections and other records are filtered.

Anti-Virus

It is almost utilization and what substance sifting is in put.

Internet

It is a living document that provides guidelines for your organization's social media use.

Social media policy

It ought to clearly recognize how the arrangement will be implemented and how security breaches and/or wrongdoing will be dealt with.

Security policies

It talks about what in the event that any Network Security Intrusion Detection or Prevention Framework is utilized and how it is executed.

Intrusion Detection

Expired credit cards, visas, passports, and IDs.

Shred

Is the act or process of throwing away or getting rid of documentation

Disposal & Destruction

It is also sometimes considered an act of Internet terrorism where terrorist activities.

Cyberterrorism

It is unsolicited usually commercial messages sent to a large number of recipients or posted in a large number of places

Spam

It can lead to a tremendous drop in guests of websites.

URL hijacking

This strategy ordinarily depends on the trusting nature of the individual being assaulted.

Social Engineering

It is often a chain message telling recipients to forward the mail to all their contacts.

Hoax

An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

Shoulder surfing

It is spontaneous as a rule commercial messages sent to a huge number of beneficiaries or posted in an expansive number of places

Spam

It is type of phishing attacks that try to lure victims via voice calls.

Vishing

It can be defined as defacing the digital assets of a company or individual to cause nuisance or permanent damage.

Electronic vandalism

It particularly targets senior administration that hold control in companies, such as the CEO, CFO, or other administrators

Whaling

These are attacks against an opening left in a functional piece of software that allows access into a system or software application without the owner's knowledge.

Backdoor Attacks

It can also install additional software, which can redirect your web browser to other sites or change your home page.

Spyware

It is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel or, less commonly, libraries or applications.

Rootkits

These were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file

Viruses

Sara, a hacker, is completing a website form to request a free coupon. The site has a field that limits the request to 3 or fewer coupons. While submitting the form, Sara runs an application on her machine to intercept the HTTP POST command and change the field from 3 coupons to 30. Which of the following was used to perform this attack?

XML injection

It is a software program designed to provide a user with administrator access to a computer without being detected.

Rootkits

It attacks are often facilitated by social engineering attacks which lure the user to a fake site.

Man In the Middle

A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

Spyware

Two programmers write a new secure application for the human resources department to store personal identifiable information. The programmers make the application available to themselves using an uncommon port along with an ID and password only they know. This is an example of which of the following?

Backdoor

These are a critical segment of a pentest in which preparation can make a major impact on the success of a pentest.

Password attacks

It is also known as bluehacking.

Bluejacking

It is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs

Bluejacking

It is an invasion where somebody tries to take data that computers, smartphones, or other gadgets transmit over a organize.

Eavesdropping Attacks

It is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Denial-of-service attack

Which of the following describes how an attacker can send unwanted advertisements to a mobile device?

Bluejacking

It is a wireless access point that has been installed on a secure network without explicit authorization from a local network administrator.

Rogue Access Points

A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place?

Bluejacking

Which of the following attacks allows access to contact lists on cellular phones?

Bluesnarfing

It is also called access point mapping - **War driving**

It could be a cyber-attack in which the culprit looks for to create a machine or arrange asset inaccessible to its planning clients by incidentally or inconclusively disturbing administrations of a have associated to the Web.

Denial-of-service attack

A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

Availability

The characteristic of a resource—ensuring access is restricted to only permitted users, applications, or computer systems.

Confidentiality

What does availability of data refer to?

The level of assurance that data will be available to people who need it, when they need it

What does confidentiality of data refer to

Rules which restrict access only to those who need to know

Digital Signatures provide which of the following?

Authentication

Franz is working on her university applications online, when the admissions website crashes. She is unable to turn in her application on time

Availability

Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts? **Integrity**

What isn't the objective of security? **Intrusion**

A weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.

Vulnerability

It is a physical device that an authorized user of computer services is given to ease authentication.

Security token

It can limit access to sensitive environments to normal business hours when. oversight and monitoring can be performed to prevent fraud, abuse, or intrusion.

Time of day restrictions

It is defined as the act of determining who someone or what something is.

Identification

A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during nonworking days. Which of the following should the technician implement to meet managements request? - **Time of day restrictions**

A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client-side certificate. Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory. How many authentication factors are in use by the VPN system? **3**

It also known as public key cryptography

Asymmetric encryption

It portrays the approach beneath which third-party organizations connect to your systems for the reason of executing commerce related to your company

Extranet policy

A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

Enforce mandatory vacations

It is a system that uses two authentication methods such as smart cards and a password

Multifactor authentication

It is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

Key exchange

It could be a set of rules connected by the proprietor, maker or director of a network, site, or service

Acceptable User Policy

It is a built up or official way of doing something.

Procedures

It incorporates how to handle connections, through sifting, individual utilize of the mail framework, dialect confinements, and authentic necessities

E-Mail

It could be a living report that gives rules for your organization's social media utilize.

Social media policy

It gives the IT department a method to review the changes before they are implemented.

Change management

It addresses any data that's secured against ridiculous divulgence.

Sensitive data

It requires understanding how people experience change and what they need to change successfully.

Individual change management

It is the action or process of classifying something according to shared qualities or characteristics. - **Classification**

It is the process by which a URL is wrongly removed from the search engine index and replaced by another URL.

URL hijacking

It could be an individual who picks up unauthorized get to to computer records or systems in arrange to encourage social or political closes.

Hacktivists

It can be current or previous representatives, temporary workers or trade accomplices that picks up get to an organization arrange, system or information and discharge this data without authorization by the organization.

Malicious insiders

It happens both exterior and interior companies and decreasing the hazard of insider information burglary at the corporate level is anything but simple

Malicious insiders

It is the act of masking a communication from an obscure source as being from a known, trusted source

Spoofing

It is additionally known as piggybacking

Tailgating

It is a growing problem for individual computer users as well as large corporations and organizations.

Data theft

Mike, a user, states that he is receiving several unwanted emails about home loans. Which of the following is this an example of?

Spam

It may be a program that can duplicate itself and infect a computer without the user's consent or information. Early viruses were usually a few forms of executable code that was hidden within the boot sector of a disk or as an executable file.

Viruses

It is a type of malware from cryptology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid

Ransomware

It does not corrupt or modify files on a target computer

Worms

It gathers your personal information and relays it to advertisers, data firms, or external users. - **Spyware**

An attacker attempted to compromise a web form by inserting the following input into the username field: admin)(|(password=*)) Which of the following types of attacks was attempted?

LDAP injection

A server is configured to communicate on both VLAN 1 and VLAN 12. VLAN 1 communication works fine, but VLAN 12 does not. Which of the following MUST happen before the server can communicate on VLAN 12?
A. The server's network switch port must be enabled for 802.11x on VLAN 12.
B. The server's network switch port must use VLAN Q-in-Q for VLAN 12.
C. The server's network switch port must be 802.1q untagged for VLAN 12.
D. The server's network switch port must be 802.1q tagged for VLAN 12.
Correct Answer: D
802.1q is a standard that defines a system of VLAN tagging for Ethernet frames. The purpose of
a tagged port is to pass traffic for multiple VLAN's
What are three of the primary security control types that can be implemented?
A. Supervisory, subordinate, and peer.
B. Personal, procedural, and legal.
C. Operational, technical, and management.
D. Mandatory, discretionary, and permanent.
Correct Answer: C
The National Institute of Standards and Technology (NIST) places controls into various types. The control types fall into three categories: Management, Operational, and Technical. Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device?
A. Authentication
B. Blacklisting
C. Whitelisting
D. Acceptable use policy
Correct Answer: C
White lists are closely related to ACLs and essentially, a white list is a list of items that are allowed To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the
PC after five minutes of inactivity. Which of the following controls is being described in this situation?
A. Management
B. Administrative
C. Technical
D. Operational
Correct Answer: C
Controls such as preventing unauthorized access to PC's and applying screen-savers that lock the PC after five minutes of inactivity is a technical control type, the same as Identification and Authentication, Access Control, Audit and Accountability as well as System and Communication Protection.

Which of the following is a management control?
A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)
Correct Answer: B
Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category. Which of the following can result in significant administrative overhead from incorrect reporting?
A. Job rotation
B. Acceptable usage policies
C. False positives
D. Mandatory vacations
Correct Answer: C
False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. This causes a significant administrative overhead because the reporting is what results in the false positives.
A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system. Which of the following describes this cause?
A. Application hardening
B. False positive
C. Baseline code review
D. False negative
Correct Answer: B
False positives are essentially events that are mistakenly flagged and are not really events to be
concerned about.
Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for
multicast
packets from the switches on the network. After investigation, she discovers that this is normal
activity for her network. Which of the following BEST describes these results?
A. True negatives
B. True positives
C. False positives
D. False negatives
Correct Answer: C

False positives are essentially events that are mistakenly flagged and are not really events to be
concerned about.
Which of the following is an example of a false negative?
A. The IDS does not identify a buffer overflow.
B. Anti-virus identifies a benign application as malware.
C. Anti-virus protection interferes with the normal operation of an application.
D. A user account is locked out after the user mistypes the password too many times.
Correct Answer: A
With a false negative, you are not alerted to a situation when you should be alerted.
A company storing data on a secure server wants to ensure it is legally able to dismiss and
prosecute staff
who intentionally access the server via Telnet and illegally tamper with customer data. Which of
the following
administrative controls should be implemented to BEST achieve this?
A. Command shell restrictions
B. Restricted interface
C. Warning banners
D. Session output pipe to /dev/null
Correct Answer: C
Within Microsoft Windows, you have the ability to put signs (in the form of onscreen pop-up
banners) that appear before the login telling similar information—authorized access only,
violators will be prosecuted, and so forth. Such banners convey warnings or regulatory
information to the user that they must "accept" in order to use the machine or network. You need
to make staff aware that they may legally be prosecuted and a message is best given via a
banner so that all staff using workstation will get notification.
Joe, a security analyst, asks each employee of an organization to sign a statement saying that
they
understand how their activities may be monitored. Which of the following BEST describes this
statement?
(Choose two.)
A. Acceptable use policy

B. Risk acceptance policy
C. Privacy policy
D. Email policy
E. Security policy
Correct Answer: AC
Privacy policies define what controls are required to implement and maintain the sanctity of data
privacy in the work environment. Privacy policy is a legal document that outlines how data
collected is secured. It should encompass information regarding the information the company
collects, privacy choices you have based on your account, potential information sharing of your
data with other parties, security measures in place, and
enforcement. Acceptable use policies (AUPs) describe how the employees in an organization
can use company systems and resources, both software and hardware.
Joe, a newly hired employee, has a corporate workstation that has been compromised due to
several visits to
P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of
such websites.
Which of the following is the BEST method to deter employees from the improper use of the
company's
information systems?
A. Acceptable Use Policy
B. Privacy Policy
C. Security Policy
D. Human Resource Policy
Correct Answer: A
Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.
Pete, a security analyst, has been informed that the development team has plans to develop an
application
which does not meet the company's password policy. Which of the following should Pete do
NEXT?

A. Contact the Chief Information Officer and ask them to change the company password policy
so that the
application is made compliant.
B. Tell the application development manager to code the application to adhere to the company's
password
policy.
C. Ask the application development manager to submit a risk acceptance memo so that the
issue can be
documented.
D. Inform the Chief Information Officer of non-adherence to the security policy so that the
developers can be
reprimanded.
Correct Answer: B
Since the application is violating the security policy, it should be coded differently to comply with
the password policy.
A major security risk with co-mingling of hosts with different security requirements is:
A. Security policy violations.
B. Zombie attacks.
C. Password compromises.
D. Privilege creep.
Correct Answer: A
The entire network is only as strong as the weakest host. Thus, with the co-mingling of hosts
with different security requirements would be risking security policy violations.
Which of the following provides the BEST explanation regarding why an organization needs to
implement IT
security policies?
A. To ensure that false positives are identified
B. To ensure that staff conform to the policy
C. To reduce the organizational risk
D. To require acceptable usage of IT systems
Correct Answer: C
Once risks have been identified and assessed then there are five possible actions that should

be taken. These are: Risk avoidance, Risk transference, Risk mitigation, Risk deterrence and
Risk acceptance. Anytime you engage in steps to reduce risk, you are busy with risk mitigation
and implementing IT security policy is a risk mitigation strategy.
Which of the following should Pete, a security manager, implement to reduce the risk of employees working in
collusion to embezzle funds from their company?
A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations
Correct Answer: D
A mandatory vacation policy requires all users to take time away from work to refresh. But not
only does mandatory vacation give the employee a chance to refresh, but it also gives the
company a chance to make sure that others can fill in any gaps in skills and satisfies the need
to have replication or duplication at all levels as well as an opportunity to discover fraud.
Two members of the finance department have access to sensitive information. The company is
concerned they
may work together to steal information. Which of the following controls could be implemented to
discover if
they are working together?
A. Least privilege access
B. Separation of duties
C. Mandatory access control
D. Mandatory vacations
Correct Answer: D
A mandatory vacation policy requires all users to take time away from work to refresh.
Mandatory vacation gives the employee a chance to refresh, but it also gives the company a
chance to make sure that others can fill in any gaps in skills and satisfies the need to have
replication or duplication at all levels. Mandatory vacations also provide an opportunity to

discover fraud. In this case mandatory vacations can prevent the two members from colluding to
steal the information that they have access to.
Mandatory vacations are a security control which can be used to uncover the following:
A. Fraud committed by a system administrator
B. Poor password security among users
C. The need for additional security staff
D. Software vulnerabilities in vendor code
Correct Answer: A
Mandatory vacations also provide an opportunity to discover fraud apart from the obvious
benefits of giving employees a chance to refresh and making sure that others in the company
can fill those positions and make the company less dependent on those persons; a sort pf
replication and duplication at all levels.
While rarely enforced, mandatory vacation policies are effective at uncovering:
A. Help desk technicians with oversight by multiple supervisors and detailed quality control
systems.
B. Collusion between two employees who perform the same business function.
C. Acts of incompetence by a systems engineer designing complex architectures as a member
of a team.
D. Acts of gross negligence on the part of system administrators with unfettered access to
system and no
oversight.
Correct Answer: D
Least privilege (privilege reviews) and job rotation is done when mandatory vacations are
implemented. Then it will uncover areas where the system administrators neglected to check all
users' privileges since the other users must fill in their positions when they are on their
mandatory vacation.
Which of the following controls has a company that has implemented a mandatory vacation
policy?
A. Risk control
B. Privacy control

C. Technical control
D. Physical control
Correct Answer: A
Risk mitigation is done anytime you take steps to reduce risks. Thus, mandatory vacation
implementation is done as a risk control measure because it is a step that is taken as risk
mitigation.
Which of the following should Joe, a security manager, implement to reduce the risk of employees working in
collusion to embezzle funds from his company?
A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations
Correct Answer: D
When one person fills in for another, such as for mandatory vacations, it provides an opportunity
to see what the person is doing and potentially uncover any fraud.
A company is looking to reduce the likelihood of employees in the finance department being
involved with
money laundering. Which of the following controls would BEST mitigate this risk?
A. Implement privacy policies
B. Enforce mandatory vacations
C. Implement a security policy
D. Enforce time of day restrictions
Correct Answer: B
A mandatory vacation policy requires all users to take time away from work to refresh. And in
the same time it also gives the company a chance to make sure that others can fill in any gaps
in skills and satisfy the need to have replication or duplication at all levels in addition to affording
the company an opportunity to discover fraud for when others do the same job in the absence of
the regular staff member then there is transparency.
The Chief Security Officer (CSO) is concerned about misuse of company assets and wishes to
determine who

may be responsible. Which of the following would be the BEST course of action?
A. Create a single, shared user account for every system that is audited and logged based upon
time of use.
B. Implement a single sign-on application on equipment with sensitive data and high-profile
shares.
C. Enact a policy that employees must use their vacation time in a staggered schedule.
D. Separate employees into teams led by a person who acts as a single point of contact for
observation
purposes.
Correct Answer: C
A policy that states employees should use their vacation time in a staggered schedule is a way
of employing mandatory vacations. A mandatory vacation policy requires all users to take time
away from work while others step in and do the work of that employee on vacation. This will
afford the CSO the opportunity to see who is using the company assets responsibly and who is
abusing it.
A software developer is responsible for writing the code on an accounting application. Another
software
developer is responsible for developing code on a system in human resources. Once a year
they have to
switch roles for several weeks.
Which of the following practices is being implemented?
A. Mandatory vacations
B. Job rotation
C. Least privilege
D. Separation of duties
Correct Answer: B
A job rotation policy defines intervals at which employees must rotate through positions.
Separation of duties is often implemented between developers and administrators in order to
separate the
following:

A. More experienced employees from less experienced employees
B. Changes to program code and the ability to deploy to production
C. Upper level management users from standard development employees
D. The network access layer from the application access layer
Correct Answer: B
Separation of duties means that there is differentiation between users, employees and duties
per se which form part of best practices.
A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They
use the same account to access each financial system. Which of the following security controls
will MOST
likely be implemented within the company?
A. Account lockout policy
B. Account password enforcement
C. Password complexity enabled
D. Separation of duties
Correct Answer: D
Separation of duties means that users are granted only the permissions they need to do their
work and no more. More so it means that there is differentiation between users, employees and
duties per se which form part of best practices.
Which of the following is the primary security concern when deploying a mobile device on a
network?
A. Strong authentication
B. Interoperability
C. Data security
D. Cloud storage technique
Correct Answer: C
Mobile devices, such as laptops, tablet computers, and smartphones, provide security challenges above those of desktop workstations, servers, and such in that they leave the office
and this increases the odds of their theft which makes data security a real concern. At a bare
minimum, the following security measures should be in place on mobile devices: Screen lock,
Strong password, Device encryption, Remote Wipe or Sanitation, voice encryption, GPS

tracking, Application control, storage segmentation, asses tracking and device access control.
A security administrator plans on replacing a critical business application in five years. Recently,
there was a
security flaw discovered in the application that will cause the IT department to manually re-enable user
accounts each month at a cost of $2,000. Patching the application today would cost $140,000
and take two
months to implement. Which of the following should the security administrator do in regards to
the application?
A. Avoid the risk to the user base allowing them to re-enable their own accounts
B. Mitigate the risk by patching the application to increase security and saving money
C. Transfer the risk replacing the application now instead of in five years
D. Accept the risk and continue to enable the accounts each month saving money
Correct Answer: D
This is a risk acceptance measure that has to be implemented since the cost of patching would
be too high compared to the cost to keep the system going as is. Risk acceptance is often the
choice you must make when the cost of implementing any of the other four choices (i.e. risk
deterrence, mitigation, transference or avoidance) exceeds the value of the harm that would
occur if the risk came to fruition.
An administrator wants to minimize the amount of time needed to perform backups during the
week. It is also
acceptable to the administrator for restoration to take an extended time frame.
Which of the following strategies would the administrator MOST likely implement?
A. Full backups on the weekend and incremental during the week
B. Full backups on the weekend and full backups every day
C. Incremental backups on the weekend and differential backups every day
D. Differential backups on the weekend and full backups every day
Correct Answer: A
A full backup is a complete, comprehensive backup of all files on a disk or server. The full

backup is current only at the time it's performed. Once a full backup is made, you have a
complete archive of the system at that point in time. A system shouldn't be in use while it
undergoes a full backup because some files may not get backed up. Once the system goes
back into operation, the backup is no longer current. A full backup can be a time-consuming
process on a large system. An incremental backup is a partial backup that stores only the
information that has been changed since the last full or the last incremental backup. If a full
backup were performed on a Sunday night, an incremental backup done on Monday night would
contain only the information that changed since Sunday night. Such a backup is typically
considerably smaller than a full backup. Each incremental backup must be retained until a full
backup can be performed. Incremental backups are usually the fastest backups to perform on
most systems, and each incremental backup tape is relatively small.
A security administrator needs to update the OS on all the switches in the company. Which of
the following
MUST be done before any actual switch configuration is performed?
A. The request needs to be sent to the incident management team.
B. The request needs to be approved through the incident management process.
C. The request needs to be approved through the change management process.
D. The request needs to be sent to the change management team.
Correct Answer: C
Change Management is a risk mitigation approach and refers to the structured approach that is
followed to secure a company's assets. Thus, the actual switch configuration should first be
subject to the change management approval.
Developers currently have access to update production servers without going through an
approval process.
Which of the following strategies would BEST mitigate this risk?
A. Incident management

B. Clean desk policy
C. Routine audits
D. Change management
Correct Answer: D
Change Management is a risk mitigation approach and refers to the structured approach that is
followed to secure a company's assets. This structured approach involves policies that should
be in place and technological controls that should be enforced.
Which of the following mitigation strategies is established to reduce risk when performing
updates to business
critical systems?
A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis
Correct Answer: C
Change Management is a risk mitigation approach and refers to the structured approach that is
followed to secure a company's assets. In this case 'performing updates to business critical
systems.
The network administrator is responsible for promoting code to applications on a DMZ web
server. Which of
the following processes is being followed to ensure application integrity?
A. Application hardening
B. Application firewall review
C. Application change management
D. Application patch management
Correct Answer: C
Change management is the structured approach that is followed to secure a company's assets.
Promoting code to application on a SMZ web server would be change management.
Which of the following MOST specifically defines the procedures to follow when scheduled
system patching
fails resulting in system outages?
A. Risk transference

B. Change management
C. Configuration management
D. Access control revalidation
Correct Answer: B
Change Management is a risk mitigation approach and refers to the structured approach that is
followed to secure a company's assets. In this case 'scheduled system patching'.
A security engineer is given new application extensions each month that need to be secured
prior to
implementation. They do not want the new extensions to invalidate or interfere with existing
application
security. Additionally, the engineer wants to ensure that the new requirements are approved by
the appropriate
personnel. Which of the following should be in place to meet these two goals? (Choose two.)
A. Patch Audit Policy
B. Change Control Policy
C. Incident Management Policy
D. Regression Testing Policy
E. Escalation Policy
F. Application Audit Policy
Correct Answer: BD
A backout (regression testing) is a reversion from a change that had negative consequences. It
could be, for example, that everything was working fine until you installed a service pack on a
production machine, and then services that were normally available were no longer accessible.
The backout, in this instance, would revert the system to the state that it was in before the
service pack was applied. Backout plans can include uninstalling service packs, hotfixes, and
patches, but they can also include reversing a migration and using previous firmware. A key
component to creating such a plan is identifying what events will trigger your implementing the

backout. A change control policy refers to the structured approach that is followed to secure a
company's assets in the event of changes occurring.
A user has received an email from an external source which asks for details on the company's
new product
line set for release in one month. The user has a detailed spec sheet but it is marked "Internal
Proprietary
Information". Which of the following should the user do NEXT?
A. Contact their manager and request guidance on how to best move forward
B. Contact the help desk and/or incident response team to determine next steps
C. Provide the requestor with the email information since it will be released soon anyway
D. Reply back to the requestor to gain their contact information and call them
Correct Answer: B
This is an incident that has to be responded to by the person who discovered it; in this case it is
the user. An incident is any attempt to violate a security policy, a successful penetration, a
compromise of a system, or any unauthorized access to information. It's important that an
incident response policy establish at least the following items: Outside agencies that should be
contacted or notified in case of an incident Resources used to deal with an incident Procedures
to gather and secure evidence List of information that should be collected about an incident
Outside experts who can be used to address issues if needed Policies and guidelines regarding
how to handle an incident Since the spec sheet has been marked Internal Proprietary
Information, the user should refer the incident to the incident response team.
Which of the following is BEST carried out immediately after a security breach is discovered?
A. Risk transference
B. Access control revalidation
C. Change management
D. Incident management
Correct Answer: D
Incident management is the steps followed when security incident occurs.

A security analyst informs the Chief Executive Officer (CEO) that a security breach has just
occurred. This
results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the
CEO asks for
further information. Which of the following strategies should be implemented to ensure the Risk
Manager and
CIO are not caught unaware in the future?
A. Procedure and policy management
B. Chain of custody management
C. Change management
D. Incident management
Correct Answer: D
incident management refers to the steps followed when events occur (making sure controls are
in place to prevent unauthorized access to, and changes of, all IT assets). The events that could
occur include security breaches.
Requiring technicians to report spyware infections is a step in which of the following?
A. Routine audits
B. Change management
C. Incident management
D. Clean desk policy
Correct Answer: C
Incident management refers to the steps followed when events occur (making sure controls are
in place to prevent unauthorized access to, and changes of, all IT assets).
Which of the following is the BEST approach to perform risk mitigation of user access control
rights?
A. Conduct surveys and rank the results.
B. Perform routine user permission reviews.
C. Implement periodic vulnerability scanning.
D. Disable user accounts that have not been used within the last two weeks.
Correct Answer: B
Risk mitigation is accomplished any time you take steps to reduce risk. This category includes

installing antivirus software, educating users about possible threats, monitoring network traffic,
adding a firewall, and soon. User permissions may be the most basic aspect of security and is
best coupled with a principle of least privilege. And related to permissions is the concept of the
access control list (ACL). An ACL is literally a list of who can access what resource and at what
level. Thus, the best risk mitigation steps insofar as access control rights are concerned, is the
regular/routine review of user permissions.
An internal auditor is concerned with privilege creep that is associated with transfers inside the
company.
Which mitigation measure would detect and correct this?
A. User rights reviews
B. Least privilege and job rotation
C. Change management
D. Change Control
Correct Answer: A
A privilege audit is used to determine that all groups, users, and other accounts have the
appropriate privileges assigned according to the policies of an organization. This means that a
user rights review will reveal whether user accounts have been assigned according to their 'new'
job descriptions, or if there are privilege creep
culprits after transfers has occurred.
A security administrator is responsible for performing periodic reviews of user permission
settings due to high
turnover and internal transfers at a corporation. Which of the following BEST describes the
procedure and
security rationale for performing such reviews?
A. Review all user permissions and group memberships to ensure only the minimum set of
permissions
required to perform a job is assigned.

B. Review the permissions of all transferred users to ensure new permissions are granted so the
employee
can work effectively.
C. Ensure all users have adequate permissions and appropriate group memberships, so the
volume of help
desk calls is reduced.
D. Ensure former employee accounts have no permissions so that they cannot access any
network file stores
and resources.
Correct Answer: A
Reviewing user permissions and group memberships form part of a privilege audit is used to
determine that all groups, users, and other accounts have the appropriate privileges assigned
according to the policies of the corporation.
Various network outages have occurred recently due to unapproved changes to network and
security devices.
All changes were made using various system credentials. The security analyst has been tasked
to update the
security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce
the number of network outages due to unauthorized changes?
A. User rights and permissions review
B. Configuration management
C. Incident management
D. Implement security controls on Layer 3 devices
Correct Answer: A
Reviewing user rights and permissions can be used to determine that all groups, users, and
other accounts
have the appropriate privileges assigned according to the policies of the corporation and their
job descriptions.
Also, reviewing user rights and permissions will afford the security analyst the opportunity to put

the principle of
least privilege in practice as well as update the security policy
After an audit, it was discovered that the security group memberships were not properly adjusted for
employees' accounts when they moved from one role to another. Which of the following has the
organization
failed to properly implement? (Choose two.)
A. Mandatory access control enforcement.
B. User rights and permission reviews.
C. Technical controls over account management.
D. Account termination procedures.
E. Management controls over account management.
F. Incident management and response plan.
Correct Answer: BE
Reviewing user rights and permissions can be used to determine that all groups, users, and
other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions since they were all moved to different roles. Control over
account management would have taken into account the different roles that employees have
and adjusted the rights and permissions of these roles accordingly.
The security administrator is currently unaware of an incident that occurred a week ago. Which
of the following
will ensure the administrator is notified in a timely manner in the future?
A. User permissions reviews
B. Incident response team
C. Change management
D. Routine auditing
Correct Answer: D
Routine audits are carried out after you have implemented security controls based on risk.
These audits include aspects such as user rights and permissions and specific events.
The system administrator has deployed updated security controls for the network to limit risk of
attack. The
security manager is concerned that controls continue to function as intended to maintain appropriate security

posture.
Which of the following risk mitigation strategies is MOST important to the security manager?
A. User permissions
B. Policy enforcement
C. Routine audits
D. Change management
Correct Answer: C
After you have implemented security controls based on risk, you must perform routine audits.
These audits should include reviews of user rights and permissions as well as specific events.
You should pay particular attention to false positives and negatives.
Which of the following security account management techniques should a security analyst
implement to
prevent staff, who has switched company roles, from exceeding privileges?
A. Internal account audits
B. Account disablement
C. Time of day restriction
D. Password complexity
Correct Answer: A
Internal account auditing will allow you to switch the appropriate users to the proper accounts
required after the switching of roles occurred and thus check that the principle of least privilege
is followed.
A system administrator has concerns regarding their users accessing systems and secured
areas using
others' credentials. Which of the following can BEST address this concern?
A. Create conduct policies prohibiting sharing credentials.
B. Enforce a policy shortening the credential expiration timeframe.
C. Implement biometric readers on laptops and restricted areas.
D. Install security cameras in areas containing sensitive systems.
Correct Answer: C
Biometrics is an authentication process that makes use of physical characteristics to establish
identification. This will prevent users making use of others credentials.

Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE)
for a $5,000
server, which often crashes. In the past year, the server has crashed 10 times, requiring a
system reboot to
recover with only 10% loss of data or function. Which of the following is the ALE of this server?
A. $500
B. $5,000
C. $25,000
D. $50,000
Correct Answer: B
SLE × ARO = ALE, where SLE is equal to asset value (AV) times exposure factor (EF); and
ARO is the
annualized rate of occurrence.
(5000 x 10) x 0.1 = 5000
An advantage of virtualizing servers, databases, and office applications is:
A. Centralized management.
B. Providing greater resources to users.
C. Stronger access control.
D. Decentralized management.
Correct Answer: A
Virtualization consists of allowing one set of hardware to host multiple virtual Machines and in
the case of software and applications; one host is all that is required. This makes centralized
management a better prospect.
A system administrator has been instructed by the head of security to protect their data at-rest.
Which of the following would provide the strongest protection?
Incorporating a full-disk encryption system
Several departments within a company have a business need to send high volumes of confidential information to customers via email.
Which of the following is the BEST solution to mitigate unintentional exposure of confidential
information?
Employ encryption on all outbound emails containing confidential information.

After recovering from a data breach in which customer data was lost, the legal team meets with
the Chief Security Officer (CSO) to discuss ways to better protect the privacy of customer data.
Which of the following controls support this goal?
Encryption and stronger access control
A security audit identifies a number of large email messages being sent by a specific user from
their company email account to another address external to the company. These messages
were sent prior to a company data breach, which prompted the security audit. The user was one
of a few people who had access to the leaked data. Review of the suspect's emails show they
consist mostly of pictures of the user at various locations during a recent vacation. No suspicious activities from other users who have access to the data were discovered.
Which of the following is occurring?
The user is using steganography.
A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop, they notice several
pictures of the employee's pets are on the hard drive and on a cloud storage network. When the
analyst hashes the images on the hard drive against the hashes on the cloud network, they do
not match.
Which of the following describes how the employee is leaking these secrets?
Steganography
Which of the following functions provides an output which cannot be reversed and converts data
into a string of characters?
Hashing
A software developer wants to prevent stored passwords from being easily decrypted. When the
password is stored by the application, additional text is added to each password before the
password is hashed. This technique is known as:
Salting
Which of the following concepts describes the use of a one-way transformation in order to

validate the integrity of a program?
Hashing
The security administrator is implementing a malware storage system to archive all malware
seen by the company into a central database. The malware must be categorized and stored
based on similarities in the code.
Which of the following should the security administrator use to identify similar malware?
Fuzzy hashes
An Information Systems Security Officer (ISSO) has been placed in charge of a classified
peer-topeer network that cannot connect to the Internet. The ISSO can update the antivirus
definitions manually, but which of the following steps is MOST important?
The signatures must have a hash value equal to what is displayed on the vendor site.
Which of the following would a security administrator use to verify the integrity of a file?
Hash
Sara, a security administrator, manually hashes all network device configuration files daily and
compares them to the previous days' hashes.
Which of the following security concepts is Sara using?
Integrity
Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long.
Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?
SHA1
Company A submitted a bid on a contract to do work for Company B via email. Company B was
insistent that the bid did not come from Company A. Which of the following would have assured
that the bid was submitted by Company A?
Digital Signatures
An email client says a digital signature is invalid and the sender cannot be verified.
Which of the following concepts is the recipient concerned with?
Integrity
A software firm posts patches and updates to a publicly accessible FTP site. The software firm
also posts digitally signed checksums of all patches and updates. The firm does this to address:

Integrity of downloaded software.
It is important to staff who use email messaging to provide PII to others on a regular basis to
have confidence that their messages are not intercepted or altered during transmission. Which
of the following types of security control are they concerned about?
Integrity
Matt, a security administrator, wants to ensure that the message he is sending does not get
intercepted or modified in transit.
Which of the following concepts relates this concern to?
Integrity
Which of the following is used by the recipient of a digitally signed email to verify the identity of
the sender?
Sender's public key
Digital signatures are used for ensuring which of the following items? (Choose two.)
Integrity & Non-Repudiation
Joe, a user, wants to send an encrypted email to Ann.
Which of the following will Ann need to use to verify that the email came from Joe and decrypt
it? (Choose two.)
Ann's private key & Joe's public key
Joe, a user, wants to send an encrypted email to Ann.
Which of the following will Ann need to use to verify the validity's of Joe's certificate? (Choose
two.)
The CA's public key & Joe's public key
A user was reissued a smart card after the previous smart card had expired. The user is able to
log into the domain but is now unable to send digitally signed or encrypted email.
Which of the following would the user need to perform?
Publish the new certificates to the global address list.
Which of the following could cause a browser to display the message below?
"The security certificate presented by this website was issued for a different website's address."
HTTPS://127.0.01 was used instead of HTTPS://localhost.
Certificates are used for: (Choose two.)
Client authentication & Code signing

Some customers have reported receiving an untrusted certificate warning when visiting the
company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate.
Which of the following could be causing the problem?
The intermediate CA certificates were not installed on the server.
Which of the following can be used to ensure digital certificates? (Choose two.)
Confidentiality & Non-repudiation
A certificate used on an e-commerce web server is about to expire.
Which of the following will occur if the certificate is allowed to expire?
Clients will be notified that the certificate is invalid.
An administrator has successfully implemented SSL on srv4.comptia.com using wildcard
certificate *.comptia.com, and now wishes to implement SSL on srv5.comptia.com.
Which of the following files should be copied from srv4 to accomplish this?
certificate, private key, and intermediate certificate chain
An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she
never sent the message.
Which of the following aspects of PKI BEST ensures the identity of the sender?
Non-repudiation
Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group.
Which of the following would prevent her from denying accountability?
Non Repudiation
A company recently experienced data loss when a server crashed due to a midday power
outage.
Which of the following should be used to prevent this from occurring again?
Redundancy
Matt, a security consultant, has been tasked with increasing server fault tolerance and has been
given no budget to accomplish his task.
Which of the following can Matt implement to ensure servers will withstand hardware failure?
RAID
After a company has standardized to a single operating system, not all servers are immune to a
well-known OS vulnerability.
Which of the following solutions would mitigate this issue?

Patch management system
A security manager requires fencing around the perimeter, and cipher locks on all entrances.
The manager is concerned with which of the following security controls?
Safety
A cafe provides laptops for Internet access to their customers. The cafe is located in the center
corridor of a busy shopping mall. The company has experienced several laptop thefts from the
cafe during peak shopping hours of the day. Corporate has asked that the IT department
provide a solution to eliminate laptop theft.
Which of the following would provide the IT department with the BEST solution?
Attach cable locks to each laptop
A business has set up a Customer Service kiosk within a shopping mall. The location will be
staffed by an employee using a laptop during the mall business hours, but there are still concerns regarding the physical safety of the equipment while it is not in use.
Which of the following controls would BEST address this security concern?
Locking cabinets
Although a vulnerability scan report shows no vulnerabilities have been discovered, a subsequent penetration test reveals vulnerabilities on the network.
Which of the following has been reported by the vulnerability scan?
False negative
Which of the following documents outlines the technical and security requirements of an agreement between organizations? - **ISA**
A large bank has moved back office operations offshore to another country with lower wage costs in an attempt to improve profit and productivity. Which of the following would be a customer concern if the offshore staff had direct access to their data? - **Privacy considerations**
Which of the following are examples of detective controls? - **Motion sensors, intruder alarm and audit.**
An organization processes credit card transactions and is concerned that an employee may intentionally email credit card numbers to external email addresses.
Which of the following technologies should this company consider? - **DLP**
Which of the following, if properly implemented, would prevent users from accessing files that are unrelated to their job duties? (Choose two.) - **Separation of duties & Least privilege**
Which of the following helps to establish an accurate timeline for a network intrusion? - **Analyzing network traffic and device logs**

A recent audit has revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Choose two.)
Disable unnecessary services &
Change default passwords
Joe is the accounts payable agent for ABC Company. Joe has been performing accounts payable function for the ABC Company without any supervision. Management has noticed several new accounts without billing invoices that were paid.
Which of the following is the BEST management option for review of the new accounts?- **Mandatory vacation**
A company hosts its public websites internally. The administrator would like to make some changes to the architecture. The three goals are: reduce the number of public IP addresses in use by the web servers, drive all the web traffic through a central point of control, and mitigate automated attacks that are based on IP address scanning. Which of the following would meet all three goals? - **Reverse proxy**
The IT department noticed that there was a significant decrease in network performance during the afternoon hours. The IT department performed analysis of the network and discovered this was due to users accessing and downloading music and video streaming from social sites. The IT department notified corporate of their findings and a memo was sent to all employees addressing the misuse of company resources and requesting adherence to company policy. Which of the following policies is being enforced? - **Acceptable use policy**
A computer security officer has investigated a possible data breach and has found it credible. The officer notifies the data center manager and the Chief Information Security Officer (CISO). This is an example of: - **escalation and notification.**
A company would like to take electronic orders from a partner; however, they are concerned that a non-authorized person may send an order. The legal department asks if there is a solution that provides non-repudiation. Which of the following would meet the requirements of this scenario? - **Digital signatures**
It gives rules with respect to remote access points and the administration by ITS of 802.11X and related remote guidelines get to - **Wireless standards policy**
Every paper or electronic record has a specific amount of time that it needs to be kept. - **Retention**
It is the act or method of storing something for future use. **- Storage**
It could be a set of rules outlined to upgrade computer security by empowering clients to utilize solid passwords and utilize them appropriately. - **Password policy**
It may be a strategy utilized to pick up get to to information, frameworks, or systems, basically through deception - **Social Engineering**

At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe? - **Tailgating**
Which of the following attacks targets high level executives to gain company information? - **Whaling**
It is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or Intimidation. - **Cyberterrorism**
It is additionally known as piggybacking. - **Tailgating**
It is the process by which a URL is wrongly removed from the search engine index and replaced by another URL. - **URL hijacking**
It is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder **- Shoulder surfing**
It is a self-replicating program that copies itself to other computers over the network without the need for any user intervention. - **Worms**
It will continue to spread and infect devices even if its signature changes to avoid detection - **Polymorphic Malware**
Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company? **- Logic bomb**
A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe? - **Buffer overflow**
Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users? - **Evil twin**
It may be a sort of assault where the aggressor breaks into the communication between the endpoints of an arranged association. - **Man-in-the-Middle Attacks**
It is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. - **Clickjacking**
It is also known as black hole DNS - **Sinkhole Attacks**
Keystroke dynamics has been used to strengthen password-based user authentication systems by considering the typing characteristics of legitimate users
Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.
Encryption is a process which transforms the original information into an unrecognizable form.
Decryption is a process of converting encoded/encrypted data in a form that is

readable and understood by a human or a computer.
Cipher is a system of writing that prevents most people from understanding the message.
Stream ciphers create an arbitrarily long stream of key material, which is combined with plain text bit-by-bit or character-by-character.
Block cipher takes a block of plain text and a key, and outputs a block of ciphertext of the same size.
Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only
MD5 – (Message Digest)
SHA – (Secure Hash Algorithms)
NTLM versions 1 and 2 – New Technology LAN Manager
RIPEMD - RACE Integrity Primitives Evaluation Message Digest
HMAC - Hash-based Message Authentication Code
An **encryption key** is a random string of bits created explicitly for scrambling and unscrambling data.
Symmetric encryption uses a single key to encrypt and decrypt data. Therefore, it is also referred to as secret-key, single-key, shared-key, and private-key encryption.
Asymmetric encryption, also known as public key cryptography, uses two mathematically related keys.
Key exchange (also key establishment) is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.
DIGITAL SIGNATURE is a process that guarantees that the contents of a message have not been altered in transit.
A **SESSION KEY** is an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computer.
KEY STRETCHING is the practice of converting a password to a longer and more random key for cryptographic purposes such as encryption.

Security policy is a definition of what it means to be secure for a system, organization or other entity.
Policy statement - Formal document outlining the ways in which an organization intends to conduct its affairs and act in specific circumstances.
Standards - a level of quality or attainment.
Guidelines - a general rule, principle, or piece of advice.
Procedures - an established or official way of doing something.
All security policies should include a well-defined security vision for the organization.

Enforcement – This section should clearly identify how the policy will be enforced and how security breaches and/or misconduct will be handled.
User Access to Computer Resources – This section should identify the roles and responsibilities of users accessing resources on the organization's network.
Security Profiles – This section should include information that identifies how security profiles will be applied uniformly across common devices
Sensitive data — This section addresses any information that is protected against unwarranted disclosure.
Passwords – This section should state clearly the requirements imposed on users for passwords.
E-Mail – This section includes how to handle attachments, through filtering, personal use of the e-mail system, language restrictions, and archival requirements
Internet – This section is about usage and what content filtering is in place.
Anti-Virus – This section identifies the frequency of updating the file definitions as well as how removable media, e-mail attachments and other files are scanned
Back-up and Recovery – A comprehensive back-up and recovery plan is included here.
Intrusion Detection – This section discusses what if any Network Security Intrusion Detection or Prevention System is used and how it is implemented.
Remote Access – This section should identify all the ways that the system can be remotely accessed and what is in place to ensure that access is from only authorized individuals
Information Security Auditing – How are all the security programs reviewed and how frequently
Information Security Training – Training occurs in many different flavors. One of the types of training required in an organization is Awareness Training
AUP – Acceptable User Policy - or fair use policy, is a set of rules applied by the owner, creator or administrator of a network, website, or service.
Privacy policy - is a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data.
Audit policy defines account limits for a set of users of one or more resources.
Extranet policy - this document describes the policy under which third-party organizations connect to your networks for the purpose of transacting business related to your company.
Password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.
Wireless standards policy - provides guidelines regarding wireless access points and the management by ITS of 802.11X and related wireless standards access.
Social media policy is a living document that provides guidelines for your organization's social media use.

Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts.
System architecture - is the conceptual model that defines the structure, behavior, and more views of a system
Change documentation should describe the requirements driving the change in sufficient detail to allow approvers and other officials to make an informed decision on the change request.
Log is an official record of events during the operation
Inventories is a complete list of items such as property, goods in stock, or the contents of a building.

A **CHANGE MANAGEMENT** system will record what changes are made.
Classification is the action or process of classifying something according to shared qualities or characteristics
Every paper or electronic record has a specific amount of time that it needs to be kept. This is called a **retention period.**

Stored cross-site scripting (Stored XSS) arises when an application receives data from an untrusted source and includes that data within its later HTTP responses in an unsafe way
Reflected cross-site scripting (Reflected XSS) arises when an application receives data in an HTTP request and includes that data within the immediate response in an unsafe way.
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSR
Fuzz testing (fuzzing) is a quality assurance technique used to discover coding errors and security loopholes in software, operating systems or networks
Encryption - is a process through which some or all of the Internet activity initiated from a Web browser is natively encrypted.
Proxy server - is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources.
Web content - is the textual, visual, or aural content that is encountered as part of the user experience on websites.
Defense in depth (layered security) is a concept in which multiple layers of security are used to defend assets.
Site security deals with securing the physical premises.
Data Security is a process of protecting files, databases, and accounts on a network.
Data Security Vulnerabilities:
❑Increased cloud computing
❑Lack of restricted access to data systems

❑Lack of user awareness

Direct-attached storage (DAS) is computer storage that is connected to one computer and not accessible to other computers.

Network-Attached Storage (NAS) is usually attached to your computer through ethernet port via router or a network switch and allow multiple computers to connect to your NAS device at the same time.

Storage area network (SAN) or storage network is a Computer network which provides access to consolidated, block-level data storage.

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disable in BIOS.

Hardware Security Module - It provides a fast solution for the for large asymmetrical encryption calculations and is much faster than software-based cryptographic solution.

Permissions:
- Who can read or change data in a file or folder.
- Implemented at individual file and folder level.

ACLs:
- Who can access files and folders.
- Implemented as MAC address filters on wireless routers and wireless APs

Hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas

A **trusted computing base (TCB)** refers to all of a computer system's hardware, firmware and software components that combine to provide the system with a secure environment.

Security Baseline defines a set of basic security objectives which must be met by any given service or system

Software Updates
Patches - Supplemental code
Hotfixes - Address specific security flaws
Rollups - Collection of patches and hotfixes
Service Packs - Comprehensive updates with new features

Logging - A log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software

Auditing - Site security also provides the ability to audit activities within the facility. This can be done through reviewing camera footage, badge reader logs, visitor registration logs, or other mechanisms

Antimalware (anti-malware) is a type of software program designed to prevent, detect and remove malicious software (malware) on IT systems, as well as individual computing devices.

It works by manipulating a vulnerable web site so that it returns malicious JavaScript to users. - **Cross-site scripting**

The handle of making apps more secure by finding, settling, and improving the security of apps. - **Application security**

The phone is the most excellent defense against this sort of assault, particularly in case coupled with a helplessness administration program. - **Application security**

It should happen as early as possible in the data flow, preferably as soon as the data is received from the external party. **- Input Validation**

It is a strategy for managing patches or upgrades for software applications and technologies. A patch management plan can help a business or organization handle these changes efficiently. **- Patch management**

It is an area of systems management that involves acquiring, testing and installing multiple patches, or code changes, to an administered computer system. - **Patch management**

It is a specialized, high-speed network that provides block-level network access to storage. - **Storage area network**

It is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. **- Cross-site request forgery**

It is computer storage that is connected to one computer and not accessible to other computers. - **Direct-attached storage**

It is a supplemental code - **patch**

It may be lasting (until fixed once more) or brief - **patch**

It characterizes a set of fundamental security goals which must be met by any given benefit or system - **security baseline**

It is used for access control, all entities are allowed access, except those listed in the blacklist - **Blacklisting**

It allows access from all items, except those included in the list. - **Blacklisting**

It can be used to find and remove spyware that has already been installed on the user's computer, or it can act much like an anti-virus program by providing real-time protection and preventing spyware from being downloaded in the first place. - **Anti-spyware**

It detects spyware through rules-based methods or based on downloaded definition files that identify common spyware programs. - **Anti-spyware**
These tools also serve for the purpose of monitoring any individual activity, the tool automatically picks the data from the linked PC that is being used by another employee who are usually the accountants and the analysts. - **Auditing**
It is a physical lock on a computer with an accompanying key used for access control or as an anti-theft system. - **cable lock**
It could be a list of things that are allowed to get to a certain framework or convention. - **White listing**
These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed. - **Protocol**
It is a hardware device which is used to connect a LAN with an internet connection. - **router**
It contains the updated table that decides where the data is transmitted or not. - **switch**
It does not broadcast the message to the entire network like the Hub. **- switch**
It continuously monitors your network, looking for possible malicious incidents and capturing information about them. - **Intrusion detection systems (IDS)**
At this layer, both the end user and the application layer interact directly with the software application. - **Application Layer**
The term can also be used as a collective noun for the press or news reporting agencies. - **Media**
It finds the destination by using logical addresses, such as IP (internet protocol). - **Network Layer**
It is the software that detects an attack on a wireless network or wireless system. - **Wireless-based Intrusion Detection System**
It characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. - **OSI Model**
It is mainly used by network administrators and security staff to monitor the operations of a network. - **Network Monitoring Systems**
It implies empowering an individual to find or learn something for themselves - **Heuristic**
It is used to transfer files between computers on a network. - **FTP**
It is a set of protocols that provides security for Internet Protocol - **Internet protocol security**

It refers to running multiple operating systems on a computer system simultaneously. - **Virtualization**

This technique is used to hide the network information of a private network while allowing traffic to be transferred across a public network like the internet. - **Network Address Translation**

A server administrator needs to administer a server *remotely* using RDP, but the specified port is closed on the outbound firewall on the network. They access the server using RDP on a port other than the typical registered port for the RDP protocol. - **SSH**

It is a name used to provide several ways that FTP software can perform secure file transfers. - **FTPS (FTP/SSL)**

It is a file transfer protocol like FTP but is much more limited. - **TFTP (Trivial FTP)**

It is a network protocol that provides file transfer and manipulation functionality over any reliable data stream. - **SFTP (SSH FTP)**

These are available either as standalone devices or as firewall components. - **Flood guards**

It serves as preventive control against denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks. - **Flood guards**

It is capable of monitoring network traffic to identify DoS attacks in progress generated through packet flooding. **- Flood guards**

It increases the efficiency of STP, RSTP, and MSTP by preventing ports from moving into a forwarding state that would result in a loop opening up in the network. **- Loop protection**

It enables an administrator configure individual switch ports to allow only a specified number of source MAC addresses ingressing the port. **- Port security**

This is a specification for a set of communication protocols to standardize the way that wireless devices can be used for Internet access. - **WAP (Wireless Application Protocol)**

802.11: There were actually two variations on the initial 802.11 wireless standard.Both offered 1 or 2 Mbps transmission speeds and the same RF of 2.4GHz.

802.11a - The first “letter” following the June 1997 approval of the 802.11 standard,this one provided for operation in the 5GHz frequency, with data rates up to 54Mbps.

802.11b - Released in September 1999, it's most likely that your first home router was 802.11b, which operates in the 2.4GHz frequency and provides a data rate up to 11Mbps
802.11g offers wireless transmission over distances of 150 feet and speeds up to 54Mbps compared with the 11Mbps of the 802.11b standard.
802.11n (Wi-Fi 4)
802.11ac (Wi-Fi 5) - Current home wireless routers are likely 802.1ac-compliant, and operate in the 5 GHz frequency space.
Maximum speed of 802.11a and 802.11g - **54 Mbps**
Maximum speed of 802.11n - **600 Mbps**
The protocol with the highest bandwidth capability is - **802.11ac (1 Gbps)**
It refers to a security access control method whereby the MAC address assigned to each network card is used to determine access to the network. **- MAC Filtering**
It protects against flooding of the Ethernet switching table, and is enabled on Layer 2 interfaces (ports). - **MAC Limiting**

It is the tool used for dividing a network into smaller parts which are called subnetworks or network segments. - **Network separation**
It is the device utilized for partitioning a arrange into smaller parts which are called subnetworks or network sections **- Network separation**
VLAN MANAGEMENT is a network switch that contains a mapping of device information to VLAN.

IMPLICIT DENY is a security stance that treats everything not given specific and selective permission as suspicious.

LOG ANALYSIS is the term used for analysis of computer-generated records for helping organizations, businesses or networks in proactively and reactively mitigating different risks.

A **wireless LAN (WLAN)** allows users to connect to a network while allowing them to remain mobile.

Wireless standards are a set of services and protocols that dictate how your Wi Fi network (and other data transmission networks) acts

Wireless security is the anticipation of unauthorized access or breaks to computers or data by means of wireless networks.

WEP was included as part of the original IEEE 802.11 standard and was intended to provide privacy.
WPA was designed as the interim successor to WEP.
WPA2 is the security method added to WPA for wireless networks that provides stronger data protection and network access control.
WPA3, released in June 2018, is the successor to WPA2, which security experts describe as “broken.

A **captive portal** is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources.

Site surveys are inspections of an area where work is proposed, to gather information for a design or an estimate to complete the initial tasks required for an outdoor activity.