

# CS205 Quiz 1 File by Tanveer Online Academy



A policy is_____.	<b>Mandatory and applies to entire organization; signed off by senior management</b>
The verizon and symantec reports show that_____.	<b>Email is the most attacked vector</b>
People, process and technology can be described as_____.	<b>Three important areas which have to be addressed for effective information security implementation</b>
During the “test/validate” stage_____.	<b>The information security team conducts a review of correctness and coverage of security control implementation</b>
Policies and procedures are the part of _____ layer in information security transformation framework.	<b>Security governance</b>
Which of the following statement is true?	<b>There are multiple players in cyber security and each has a role to play to improve cyber security posture</b>
People, process, and _____are together referred to as the Information Security Triad.	<b>Technology</b>
In an IT network how data exfiltration can be avoided at edge?	<b>Through network DLP solution</b>
The purpose of the information security lifecycle is to ensure that_____.	<b>All security projects &amp; activities consistently follow the same sequence and steps</b>
What information needs to be backed up in an enterprise IT?	<b>All of the above</b>

Layer 2 of the security transformation model emphasis on_____.	Identifying vulnerabilities through a risk-based approach
The typical enterprise IT network has been characterized to help in understanding_____.	IT components, architecture of the network, and security devices and placement
Security hardening can best be described as_____.	Configuring it assets to maximize security and minimize risk
The DMZ is an important zone in the network with the following functions:	Allowing external access to important services such as web, email, and remote access, while providing a layer of protection and filtering
How high availability can be designed in an enterprise IT network?	All of given
What is the advantage of offsite backup in an enterprise IT network?	Data will be preserved in case of some catastrophic event
People, process, and technology together form_____.	A holistic approach to information security
_____ assigns quantifiable measures.	Standard
How is information security implemented?	With the help of an information security program
Authentication, access control, data confidentiality, data integrity, non-repudiation, availability are covered by_____.	Security service
IT/ Infosec Teams require information security project report at _____ basis.	Daily
he IT global cyber security index (GCI) is_____.	An initiative that covers five main areas in order to assist governments improve their cyber security posture.
Which of the following programs is relevant when we are simply trying to “focus attention on security”?	Security education
One of the challenges in effective implementation of a security transformation project in a small-sized organization is_____.	Adhoc culture and lack of discipline
What are the performance KPIS of IT teams?	Both a & b
The impact of vm sprawl is that_____.	Vms can be created quickly, self-provisioned, or moved between physical servers, leading to too many vm's

The IT global cyber security index (GCI) is_____.	<b>An initiative that covers five main areas in order to assist governments improve their cyber security posture.</b>
Security governance simply means_____.	<b>Managing the security program</b>
_____ is the part of Information Security Awareness.	<b>Training</b>
What is the best description of a security standard or framework?	<b>Blue print or roadmap for achieving information security objectives</b>
What is disaster recovery (DR) in an enterprise IT network?	<b>A pre planned approach for establishing it functions at alternate site</b>
The ITU global cyber security index (GCI) covers:	<b>Legal, technical, organizational, capacity building and cooperation</b>
Layer 2 of the security transformation model emphasis on_____.	<b>Security governance</b>
For effective information security implementation, the security journey should start with_____.	<b>Management commitment</b>
One of the major challenges of information security in Pakistan is that it is_____.	<b>Not funded adequately</b>
As per ISACA, risk should be managed so that_____.	<b>There is an acceptable level of assurance and predictability to the desired outcomes of any organizational activity</b>
Security in the trenches refers to_____.	<b>Most basic security hardening activities usually carried out by junior staff</b>