

CS205 Quiz 1 File by Tanveer Online Academy



A policy is_____.	Mandatory and applies to entire organization; signed off by senior management
The verizon and symantec reports show that_____.	Email is the most attacked vector
People, process and technology can be described as_____.	Three important areas which have to be addressed for effective information security implementation
During the “test/validate” stage_____.	The information security team conducts a review of correctness and coverage of security control implementation

Policies and procedures are the part of _____ layer in information security transformation framework.	Security governance
Which of the following statement is true?	There are multiple players in cyber security and each has a role to play to improve cyber security posture
People, process, and _____ are together referred to as the Information Security Triad.	Technology
In an IT network how data exfiltration can be avoided at edge?	Through network DLP solution
The purpose of the information security lifecycle is to ensure that _____.	All security projects & activities consistently follow the same sequence and steps
What information needs to be backed up in an enterprise IT?	All of the above
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 _____.	An initiative that covers five main areas in order to assist governments improve their cyber security posture.

Security governance simply means_____.	Managing the security program
_____is the part of Information Security Awareness.	Training
What is the best description of a security standard or framework?	Blue print or roadmap for achieving information security objectives
What is disaster recovery (DR) in an enterprise IT network?	A pre planned approach for establishing it functions at alternate site
The ITU global cyber security index (GCI) covers:	Legal, technical, organizational, capacity building and cooperation
Layer 2 of the security transformation model emphasis on_____.	Security governance
For effective information security implementation, the security journey should start with_____.	Management commitment
One of the major challenges of information security in Pakistan is that it is_____.	Not funded adequately
As per ISACA, risk should be managed so that_____.	There is an acceptable level of assurance and predictability to the

	desired outcomes of any organizational activity
Security in the trenches refers to_____.	Most basic security hardening activities usually carried out by junior staff
During the third stage (remediation plan) of the information security lifecycle, the following activities are planned and prepared.	Methodology/framework, controls, resources, timeline, approvals, sop
The 4 layer security transformation model and isms requirements and controls_____.	May form essential elements of the security program
It would be correct to say that the security posture in Pakistan can be improved by_____.	Effective actions taken by regulators, organizations, and building an effective cyber security eco-system
Regionally, the most well developed cyber security strategy and framework developed by Singapore by ITU is at rank_____.	1
What are the three types of redundant site models in an enterprise network?	Hot site, cold site and warm site
A _____ is a blueprint or roadmap for achieving Information Security objectives	Standard

What are the famous SIEM solutions available in market?	OSSEC, SPLUNK AND Q-RADAR
In Global Cyber Security Index 2017 (ITU) Pakistan at ranked_____.	67th
In information security life cycle methodology and framework phase comes in _____step.	Remediation Plan
An information security program is_____.	The sum total of all security activities planned and executed by the organization
The purpose of network admission control (NAC) is to allow only compliant systems to connect to the network through the following IEEE standard_____.	IEEE802.1X
Iso27001:2013 (isms) clause 5.1 talks about_____.	Policy and objectives, integration into processes, resources, communication, promoting continual improvement, intended outcomes
Which of the following statements is false?	Iso27001:2013 has ten short clauses and a long annex with 14 sections, and 113 controls

What do you mean by RTO in a business continuity plan?	Maximum age of files that an organization must recover from backup storage for normal operations to resume after disaster
There are _____ main pillars of information security.	3
Information security management committee requires information security project report at _____ basis.	Weekly
The information security transformation model:	Four layers, with the first layer being on the bottom: security hardening
_____ are important tasks where the information security manager should be involved.	Signing off critical change requests, monitoring the vulnerability management program, facilitate incident management process
The key factor related to cloud, mobile, IOT, and social is that_____.	It has further complicated the already difficult task of achieving a strong security posture

Information security management committee requires information security project report at _____basis.	Weekly
_____ refers to potential damage or loss.	Risk