1) The ciso should be able to complement his own technical knowledge by. Building a good team
2) In a medium-sized security organization in Pakistan , it is likely the number of security staff will be 10-15 / 2-4 / 5-10
3) What was the old name of iso27002:2013 standard, iso17799
4) In which format result of penetration testing should be documented. Machine readable standard
5) Which of the following are the sub controls of communication security. Event logging control
6) At which phase information security lifecycle information security become integral part. Maintenance phase
7) The total number of discretionary controls in appendix a5 through a18 are, 114
8) While implementing the 4-layer security transformation model. It is suggested to have a high level and minimal policy in place
9) According to this module, the main function of the ciso is to conduct the following for the security program -------
review, monitor, and propose
10) In a large sized security organization, the following security function are likely to be found, engineering, operation, governance, and framework/standards
11) How can organization ensure protection of assets that are accessible by suppliers by signing contracts with only known suppliers
12) Security governance may be considered as, a function lying above the it governance framework
13) Procedure can best be describe as, detailed step by step instruction to archive a given goal or mandate
14) The ' Disciplinary process ' is a control belonging to which section in the isms appendix, A.7.2.3
15) Guideline should be, pasted on the company notice board for easy visibility
16) Iso27001:2013 (isms) has how many mandatory initial clauses , 10
17) Which of the following activity should be performed to test organization readiness to identify and stop attack or to respond quickly and effectively , Periodic red team exercise
18) As per iso27001(20130 how information security incident should be responded? Inform the incident handling team
19) Each person with administrator account should be authorized by? System administrator
20) What should an organization do to control access to sensitive information on need to know bases?
Locate all sensitive information on separate vans
21) While policy is recommended by data protection control of cis for mobile device usage in an organization?
Hard drive of mobile devices should be encrypted
22) Frequency of running automated valverability scanner against all sestem on a network in an enterprise should be? Weekly
23) As per malware defense control why DNS query logging should be enabled ?
to detect host name lookup for known malicious domains
24) Why should we use scop validated vulnerability scanner?
Because it looks for both cade based and configuration based vulnerability
25) After getting vulnerability scanning results patches should be applied to? All the system throughout the organization
26) Which of the following system configuration management tool is used for Linux system? Active directory
27) Boundary defense control comes under which category of cis critical controls? Foundational control
28) Automated configuration monitoring tools should compliant with which protocol to streamline reporting? Scap
29) Why cis recommend to configure monitoring system in an organization network?
To record the network packets passing through the boundary
30) If a system in an organization gets compromised, how can we prevent an attaker to compromised the neighboring system?
Through network based intrusion prevention system (IPS)
31) Centrally managed anti-malware software should be used in an organization to,
continuously monitor and defend organizations servers and workstations
32) Which of the following tool can be used to enforce access controls to data? Host-based data loss prevention (dlp)
33) From which type of system URL request should be logged in ordered to identify potentially malicious activity?
On-site devices
34) Which cis control is described in this module? Wireless access control
35) As per malware defense control why DNS query logging should be enabled?
To detect host name lookup for known malicious domain
36) When vulnerability scan run and report is generated and shared with respective resource , which vulnerability they should fix an priority basis? Critical risk vulnerability

37) What should an organization do to control access to sensitive information on need-to-know basis?
Locate all sensitive information on separate vlans

38) If multi factor authentication is not supported then user account shall be required to? Use password longer than 14 characters

39) As per cis framework what is the best practice to store logs generated from system?
Aggregates log to a central management system

40) Why security engenering is placed at layer 3 of transformation model?
Consist of complicated security activities which take more time and effort

41) Automated tool should be used to verify and compare the network devices configuration with approved security configuration

42) What should a system do whenever an administrater account is added or removed? Issue a log entry and alert

43) Wireless access control comes under which category of cis top 20 controls? (18) Basic / Advanced / foundation

44) In an enterprise which software should be allowed to install and execute? Software included in whitelist

45) As per cis homework what is the best practice to store logs generated from system?
Store logs on the same machine which generate

46) Which of the following can be used to look for unusual attack mechanism on organization network boundaries?
Network based intrusion detection (ids) sensor

47) Before deploying any new devices in an networked environment what should be done with password?
Change the default password

48) COBIT has ------ enablers and ------- principles. 7 , 5

49) Which of the following programs is relevant when we are simplify trying to "focus attention on security"? security education

50) IT/Infosec team requires information security project report at ------- bases. Daily / weekly

51) which of the following protocol are used for remote administration of a system. TCP/UDP

52) a policy is ------ Mandatory and applies to entire organization , singed off by senior management

53) an information security program is -----
the sum to of all security audit and assessment activities planned and executed by management

54) the DMZ is an important zone in the network with the following function Allowing external access to important services as web email, and remote access , while providing the layer of protection and filtering

55) Anthem insurance breach 2014 was initiated through? Phishing email

56) How many TCP and UDP ports are scanned in a default scan? 1900 TCP pots and 180 UDP ports

57) STIG stands for ------- security technical implementation guide

58) The ITU global cyber security index (GCI) covers: legal, technical, organizational, capacity building and cooperation

59) Against which framework NESSUS scanner gives configuration auditing feature? CIS and DISA

60) The antivirus program must be configured to update signature files on a .... basis. Daily

61) Which of the following scan is deeper and gives more detailed scanning result? Credential vulnerability scanning

62) Which of the following modules are displayed on home screen of qualys trial version?
Vulnerability management and policy compliance

63) What do you mean by RTO in a business continuity plan? max amount of downtime an organization can handle

64) What do you mean by RPO minimum frequency of backups

65) What type of IT assets do not have a CIS/DISA STIG ?
– Software applications (ASP.NET, PHP, Other) – Other applications such as asterisk deployments

66) What contents a DISA STIG covers? General information , discussion, check content, fix test, cci

67) Which of the following function is performed by IT operation team in vulnerability management process?
Takes backup and downtime / run vulnerability scanner

68) Security governance simply means ------------- Managing the security program

69) A guideline ----------- a statement of best practice that further elaborates the procedure/sop

70) Checklist of applicable security controls steps includes? Make a checklist for progress tracking and share with it team

71) Which of the following polices NESSUS can scan for compliance? CIS benchmarks

72) The information security transformation framework is recommended for ------------ information security governance

73) During the 3rd satge of the information security lifecycle, the following activities are planed and prepared.
Methodology/framework, controls resources, timeline, approvals, sop

74) Which team test the patches in test environment in vulnerability management process? IT operation team
75) Which types of plugins are supported by NESSUS scanner? CIS and DISA
76) Which one of the following is considered the first step in a vulnerability scan? Checking if the remote host is alive
77) How many individuals were affected in anthem insurance breach 2041? 78.8 million
78) Which of the following tools are offered free QUALYS? Browser check
79) Which subscription service model QUALYS offer? Annual subscription
80) Which best practices are to be followed for applying security patches? All the updates are necessary to install and working backup
81) Which of the following statement is correct? NVD is superset of CVE
82) Policy and compliance of "governances " function of software assurance maturity model is focused on ……
understanding and meeting external legal and regulatory requirements
83) What information we get from open TCP and UDP parts? Whether host is alive or not
84) Which activities are carried out at stage 1 of transformation model? All of the given
85) What is the first step in running a policy compliance scan through QUALYS? Add ip address of scan
86) Which of the following security practices come under "construction" function of software assurance maturity modal?
Threat assessment , security requirements, security architecture
87) What features set QUALYS scanner offers? Cloud base service
88) As per Carnegie mellon university computing consortium commercial software contains?
20 to 30 bugs for every 1000 lines of code
89) How to security of outsourced services can be evaluated? Ask for 3rd party security review
90) Which of the following are common vulnerability scanners? Nessus, rapid7, Openvas and QUALYS
91) Which screen is displayed immediately after login screen in NESSUS scanner ? Vulnerability management screen
92) How can an authorized wireless access point connected to a wired network can be detected and alerts can be generated?
Through network vulnerability scanning tools
93) As per cis critical controls from how many minimum synchronized time resources all networks devices and servers should retrieve time? 3
94) The dedicated machine used by administrators for administrative tasks should have following features,
isolated from organization primary network
95) How can an authorized wireless access point connected to a wired network can be detected?
Through wireless intrusion detection system
96) Which of the following cis critical control is discussed in this module? Secure configuration for network devices