

Security Audit Checklist

1. Whether the firewalls exist on all inbound and outbound connections	<input type="checkbox"/>
2. Whether the firewalls are installed inside the organization network to segregate networks of different security levels	<input type="checkbox"/>
3. Whether there is a policy to allow connection from external networks	<input type="checkbox"/>
4. Whether the organization wants to hide its internal network form outsiders using a NAT or PAT	<input type="checkbox"/>
5. Whether the network devices such as firewall, IDS, and router are configured as per the security policy standards?	<input type="checkbox"/>
6. Whether there is a monitoring mechanism to check the firewall's CPU utilization from time to time	<input type="checkbox"/>
7. Whether there is a policy for managing the patches to the network resources within a fixed time period	<input type="checkbox"/>
8. Whether the patches to the network resources are tested first and then deployed to production systems	<input type="checkbox"/>
9. Whether the policy contains a better cryptographic solution that covers all the standards and regulatory controls	<input type="checkbox"/>
10. Whether there is a recorded processes and procedures for encryption keys management	<input type="checkbox"/>
11. Whether the cardholder's data is retained when there is no more business dealing with them	<input type="checkbox"/>
12. Whether the CVV2 or magnetic stripe data stored in the database or log files	<input type="checkbox"/>
13. Whether the network devices passwords are encrypted	<input type="checkbox"/>
14. Whether the sensitive data traveling through network is encrypted	<input type="checkbox"/>
15. Whether the remote system administration is performed using telnet or Rlogin	<input type="checkbox"/>
16. Whether the routers are connected to the internal systems or DMZ systems	<input type="checkbox"/>
17. Whether there is an installation of anti-virus software on network devices	<input type="checkbox"/>
18. Whether the latest anti-virus signature files are updated	<input type="checkbox"/>

19. Whether there is a data access privileges to cardholder data in the access control policies	<input type="checkbox"/>
20. Whether the firewalls are administered only by network security personnel	<input type="checkbox"/>
21. Whether there is a mechanism to authenticate all non-consumer users when accessing cardholder data	<input type="checkbox"/>
22. Whether there is an automatic account lock method implemented when users failed to provide exact credentials within six login attempts	<input type="checkbox"/>
23. Whether there is a strict password policy implemented to restrict easily guessable passwords	<input type="checkbox"/>
24. Whether all unnecessary services disabled on a server	<input type="checkbox"/>
25. Whether security controls enabled in the application development process	<input type="checkbox"/>
26. Whether source code review was performed for vulnerabilities before deploying the applications into production	<input type="checkbox"/>
27. Whether network and application resources are tested for vulnerabilities	<input type="checkbox"/>
28. Whether the event logs do contain date and timestamps for all critical services	<input type="checkbox"/>
29. Whether the event log files are reviewed regularly	<input type="checkbox"/>
30. Whether the security personnel are performing vulnerability assessments network resources regularly	<input type="checkbox"/>
31. Whether there is a file integrity checking mechanism implemented to monitor unauthorized modifications to critical data	<input type="checkbox"/>
32. Whether security alerts for the intrusions are implemented through IDS or IPS methods	<input type="checkbox"/>
33. Whether the network security controls such as firewalls, IDS, and IPS are installed with latest signatures	<input type="checkbox"/>
34. Whether there a proper training is provided to the employees on operational business and recovery plan execution responsibilities	<input type="checkbox"/>
35. Whether there a regular testing method for the disaster recovery plan (DRP) and the business contingency plan (BCP)	<input type="checkbox"/>
36. Whether roles and responsibilities of each security personnel are defined	<input type="checkbox"/>
37. Whether there is a mechanism for regular data backup for critical systems	<input type="checkbox"/>

38. Whether the data backup storage locations are secured from unauthorized access	<input type="checkbox"/>
39. Whether there is an IR plan developed and documented	<input type="checkbox"/>
40. Whether all the employees are required to sign an agreement stating that they have read and understood the policies and procedures	<input type="checkbox"/>
41. Whether there is an access to the data center restricted and closely monitored	<input type="checkbox"/>
42. Whether the functions are isolated such as administrative privileges, APIs, etc.	<input type="checkbox"/>
43. Whether proper restrictions are implemented for all the personal devices and accounts	<input type="checkbox"/>
44. Whether appropriate BYOD policies are implemented and maintained across the organization	<input type="checkbox"/>
45. Whether endpoint verification is turned on across the organizational network	<input type="checkbox"/>
46. Whether data loss prevention software installed	<input type="checkbox"/>
47. Whether a team password manager is set up and the password requirement documentation is	<input type="checkbox"/>
48. Whether a security agreement is signed by the third-party vendors for working with the organization	<input type="checkbox"/>
49. Whether the internal servers are hardened, and unnecessary applications are removed	<input type="checkbox"/>
50. Whether the server permissions are configured properly for the users	<input type="checkbox"/>
51. Whether the remote access security policy is implemented for the users	<input type="checkbox"/>
52. Whether there are group access permissions for the required users	<input type="checkbox"/>
53. Whether wireless security protocols are implemented appropriately, and the wireless network is properly configured	<input type="checkbox"/>