**Auditing IT Infrastructure for Compliance**

Name: Gaurav singh

Roll No: C\_70

LAB 1

Aim: Conduct thorough research and generate audit checklist for each framework.

**Research:**

**COSO(Committee of Sponsoring Organizations):** The COSO (Committee of Sponsoring Organizations) framework is a widely recognized and respected internal control framework used for various business processes, including IT infra auditing. In short and simple terms, the COSO framework provides a structured approach to assess and improve the effectiveness of internal controls within an organization.

In the context of IT infra auditing, the COSO framework helps auditors evaluate and enhance the controls in place to safeguard an organization's information technology infrastructure. This includes areas such as data security, system reliability, compliance with relevant regulations, and overall IT governance.

**ITIL(Information Technology Infrastructure Library**): It is a set of best practices and guidelines for IT service management (ITSM) that was developed by the United Kingdom's Office of Government Commerce (OGC) in the 1980s. ITIL provides a framework for organizations to align their IT services with their business needs, improve efficiency, and deliver better value to their customers or end-users. The framework includes a series of books or publications that cover various aspects of IT service management, such as service strategy, service design, service transition, service operation, and continual service improvement.

**Checklist:**

|  |  |  |
| --- | --- | --- |
| 1. Do firewalls exist on all Internet or Extranet connections | Yes | CC |
| 2. Are firewalls used internally to separate networks of different security levels? | No – there are no different security levels on the internal LAN | CC |
| 3. Is there a formal procedure for approving all external connections? | N/A – No External Connections Supported | CC |
| 4. Is the use of NAT or PAT implemented into your environment to hide internal network from the Internet? | Yes, ICSA-certified | CC |
| 5. Is your firewall and router configured to conform with documented security standards? | Yes | CC |
| 6. Is your firewall’s CPU utilization monitored at least every 15 minutes? | No - We use a hardware based ICSA-Certified firewall that does not allow that level of monitoring | CC |
| 7. Are available security patches implemented within 30 days? | Yes | CC |
| 8. Are security patches tested before they are deployed to production systems? | Yes | CC |
| 9. Do all system changes go through a formal change control process? | Yes | CC |
| 10. Does your cryptographic solution conform to applicable international and national standards, as well as all legal and regulatory controls? | Yes | CC |
| 11. Are only crypto devices used that meet the approval standards and policies of your organization? | Yes | CC |
| 12. Are there documented processes and procedures in place for encryption keys? | Yes | CC |
| 13. Is access to keys restricted to the fewest number of custodians necessary? | Yes | CC |
| 14. Is cardholder information retained when it is no longer needed for business reasons | Yes. The SHA1 hash of the card number (PAN) is stored for velocity checking purposes. This field is available only to the Cardease application and Administrators. | CC |
| 15. Is a quarterly inventory audit performed to verify if any stored cardholder information exceeds your retention requirements? | Yes | CC |
| 16. Is CVV2 or magnetic stripe data stored in the database or log files? | No | CC |
| 17. Are all passwords on network devices and systems encrypted? | Yes | CC |
| 18. Is stored cardholder data encrypted by one of the following, one-way cipher (hash indexes) such as SHA-1 (not MD5), Truncation, Simple ciphers, index tokens and PADS, strong cryptography such as PGP or Triple-DES with associated key management processes and procedures? | Yes | CC |
| 19. Is telnet or Rlogin used for remote system administration? | No | CC |
| 20. Is externally accessible account data transmitted in unencrypted format? | No | CC |
| 21. Is confidential account information transmitted via unencrypted email format? | No | CC |
| 22. Is strong cryptography and appropriate key controls in place to safeguard data during transmission? | Yes for all data crossing externally accessible networks | CC |
| 23. Are modems connected to the internal systems or DMZ systems? | Yes | CC |
| 24. Is anti-virus software installed on all servers and workstations? | No – for reliability reasons. However, all other machines on the network are protected by a maintained and updated Anti-virus package. Production servers do not have e-mail access and are not used as workstations thus reducing the possibility of infection. | CC |
| 25. Have anti-virus signature files been updated to the latest signature file? | N/A | CC |
| 26. Is account information access on a need to know basis only? | Yes | CC |
| 27. Are access control policies in place for data access privileges to cardholder information? | Yes | CC |
| 28. Is firewall administration limited to only the network security administration staff? | Yes | CC |
| 29. Is a unique username and password required for each non-consumer user that logs into a system containing cardholder information? | Yes | CC |
| 30. Is at least one of the following methods used to authenticate all non-consumer users when accessing cardholder information: unique user name and password? token devices (i.e., SecureID, certificates, or public key)? biometrics? | Yes | CC |
| 31. Are non-consumer users required to change their password every 60 days? | Yes | CC |
| 32. Are non-consumer user accounts locked within 6 invalid login attempts? | Yes – every 3 attempts | CC |
| 33. Are password protected screen savers or terminal locks used on all critical systems? | Yes – all machines run locked | CC |
| 34. Are group passwords allowed on critical systems? | No | CC |
| 35. Are passwords required to contain both numeric and alphabetic characters? | Yes | CC |
| 36. Are individuals allowed to submit a new password that is the same as a previous password? | No | CC |
| 37. Are all internal and external dormant accounts removed? | Yes | CC |
| 38. Are applications run on default installations of operating systems? | No | CC |
| 39. Is more than one application running as the primary function of a server at any given time? | Yes | CC |
| 40. Are the minimum hardware components met on each network component for the software to function properly? | Yes | CC |
| 41. Are all unnecessary services disabled on a server? | Yes | CC |
| 42. Are security controls built into the application development process? | Yes - Only one Developer has access to the Cardease source code and all changes are tracked using Visual SourceSafe. All source code is stored on a hardened Windows 2000 Server, access is tightly controlled and weekly reviews of the SourceSafe Change logs are performed. | CC |
| 43. Has the application code been tested for vulnerabilities prior to entering production? | Yes | CC |
| 44. Do you perform penetration testing on your network and applications at least once a year and after any significant modifications? | Yes | CC |
| 45. Is access to all audit trails logged on all critical systems? | Yes | CC |
| 46. Do you log the following: success and failed logins by all users, access to audit trails, deletion of objects, identification of affected components, root/administrator access origination and destination? | Yes – where supported by Windows 2000 | CC |
| 47. Are actions related to encryption key management logged on all servers that utilize the keys? | N/A | CC |
| 48. Do logs include date and time stamp on all critical systems? | Yes | CC |
| 49. Are audit trails on all critical systems secured in a way that they cannot be tampered with? | Yes – as supported by Windows 2000 | CC |
| 50. Do you review audit logs at least once a week on critical systems? | Yes | CC |
| 51. Are audit logs retained for at least six months on all critical systems? | Yes | CC |
| 52. Are vulnerability assessments performed on the internal and external network on a monthly basis and after updates and/or upgrades to systems? | No – external network connections are tested quarterly | CC |
| 53. Is there a file integrity monitoring system in place to alert personnel of unauthorized modifications to critical systems? | No - only an Administrator can add or modify application software on a production Server. | CC |
| 54. Are security alerts from the intrusion detection sensor monitored 24 hours a day, 7 days a week? | No | CC |
| 55. Do you have Network IDS on perimeter related systems? | N/A | CC |
| 56. Are the latest intrusion detection system (IDS) signatures installed on all IDS sensors? | N/A | CC |
| 57. Are file comparison checks being reviewed on critical systems at least once a day? | No | CC |
| 58. Is staff provided with adequate training on operational business and recovery plan execution responsibilities? | Yes | CC |
| 59. Are the disaster recovery plan (DRP) and the business contingency plan (BCP) tested annually? | Yes | CC |
| 60. Are security roles and responsibilities formally defined? | Yes | CC |
| 61. Are critical data backed up on a daily basis? | Yes | CC |
| 62. Are backup tapes stored in a location that does not require authorized access? | No | CC |
| 63. Are all associated third parties with access to cardholder data contractually required to adhere to CISP data security requirements? | No – no third party has access to cardholder data | CC |
| 64. Are information security policies documented, kept current and disseminated to all employees, vendors, contractors and partners? | Yes | CC |
| 65. Is there a security awareness and training program in place? | Yes | CC |
| 66. Are pertinent security alerts monitored, analyzed and distributed to appropriate personnel? | Yes | CC |
| 67. Is a security incident response plan formally documented? | Yes | Both |
| 68. Are employees required to sign an agreement verifying they have read and understood the polices and procedures? | Yes | CC |
| 69. Are employees with access to cardholder data permitted to begin work prior to completion of a background investigation (including credit and criminal record checks)? | CC – Yes, Parkeon – No | Both |
| 70. Is access to the data center restricted and closely monitored? | Yes | Parkeon |
| 71. Are all paper and electronic media — e.g. computer, networking, and communications hardware, telecommunications lines, etc. — containing cardholder information located in a physically secure environment? | Yes | Both |
| 72. Have all discarded media been erased or destroyed using a formal procedure that ensures the complete deletion of all sensitive data? | Yes | CC |
| 73. Do you maintain strict control over the internal and external distribution of any paper or electronic media containing cardholder data? | Yes | CC |
| 74. Are visitors, including vendors, permitted to enter data centers or access sensitive systems without an escort? | No | Parkeon |
| 75. Are visitors asked to sign out and turn in their badge or tag before leaving the building? | Yes | Parkeon |
| 76. Is a visitor log retained for at least three months to retain a log of physical activity? | Yes | Parkeon |
| 77. Are all media devices properly inventoried and securely stored? | Yes | Both |