Auditing Applications

Checklist for Auditing Applications

☐ 1. Review and evaluate data input controls.
☐ 2. Determine the need for error/exception reports related to data integrity, and evaluate whether this need has been fulfilled.
☐ 3. Review and evaluate the controls in place over data feeds to and from interfacing systems.
☐ 4. In cases where the same data are kept in multiple databases and/or systems, periodic ‘sync’ processes should be executed to detect any inconsistencies in the data.
☐ 5. Review and evaluate the audit trails present in the system and the controls over those audit trails.
☐ 6. The system should provide a means to trace a transaction or piece of data from the beginning to the end of the process enabled by the system.
☐ 7. The application should provide a mechanism that authenticates users, based at a minimum, on a unique identifier for each user and a confidential password.
☐ 8. Review and evaluate the application’s authorization mechanism to ensure that users are not allowed to access any sensitive transactions or data without first being authorized by the system’s security mechanism.
☐ 9. Ensure that the system’s security/authorization mechanism has an administrator function with appropriate controls and functionality.
☐ 10. Determine whether the security mechanism enables any applicable approval processes.
☐ 11. Ensure that a mechanism or process has been put in place that suspends user access on termination from the company or on a change of jobs within the company.
☐ 12. Verify that the application has appropriate password controls.
☐ 13. Review and evaluate processes for granting access to users. Ensure that access is granted only when there is a legitimate business need.
☐ 14. Ensure that users are automatically logged off from the application after a certain period of inactivity.
☐ 15. Evaluate the use of encryption techniques to protect application data.
☐ 16. Evaluate application developer access to alter production data.
☐ 17. Ensure that the application software cannot be changed without going through a standard checkout/staging/testing/approval process after it is placed into production.
☐ 18. Evaluate controls around code checkout, modification, and versioning.
☐ 19. Evaluate controls around the testing of application code before it is placed into a production environment.
☐ 20. Ensure that appropriate backup controls are in place.
☐ 21. Ensure that appropriate recovery controls are in place.
☐ 22. Evaluate controls around the application’s data retention.
☐ 23. Evaluate controls around data classification within the application.