Lecture 9 – Auditing Applications

Aron Kondoro

Introduction

- Business application systems
  - Computer systems used to perform & support specific business processes
  - External vendor vs custom-made
- Control depends on
  - Business process supported
  - Programming language used
  - Technology platform underneath

Steps for Auditing Applications

1. Review input controls

- Evaluate controls built into system transactions over the input of data
- How
  - Verify invalid data is rejected or edited on entry
  - Understand application purpose & identify data integrity risks
  - Discussion with developer
  - Code review
  - Examples
    - Fields intended for numbers should not allow alphanumeric entry
    - Logic checks in transactions i.e. 24 hrs/day or 60 mins/hour
    - Preventing duplicates in unique fields

2. Determine need for error reports

- Evaluate whether the need for error/exception reports has been fulfilled
- Error reports allow data integrity problems to be reviewed when input controls are inappropriate
- How
  - Discuss error & exception handling with developer or administrator
  - Identify type of anomaly reports needed
  - Look for evidence of those reports

3. Review interface controls

- Evaluate controls in place over data feeds to/from interfacing systems
- Ensure data is transmitted accurately and completely
- How
  - Identify all existing interfaces i.e. System flow diagrams, interviews
  - Determine controls i.e. Code reviews, interviews
  - Control totals i.e. Hash totals, record counts
  - Review evidence applicable error reports are reviewed and acted upon
  - Suspense files to handle the errors
  - Reconciliation reports

4. Review data consistency mechanisms

- If the same data is stored in multiple databases ensure periodic sync processes are executed to detect inconsistencies
- How
  - Review existance and effectiveness of mechanism i.e. Discussion with app developer
  - Designation of master/slave

5. Review audit trails

- Evaluate audit trails in the system and their controls
- Useful for troubleshooting breaches
- How
  - Review logging processes with developer/administrator
    - What activity was performed, original/new values, who performed the change, when it was performed
  - Evaluate storage
    - Secure storage, reasonable retainment period

6. Evaluate transaction tracing mechanisms

- Ensure system provides means of tracing transaction/data from beginning to end
- Helps to pinpoint errors or irregularities in processing
- How
  - Review application with developer or administrator
  - Identify sample of recent transactions and attempt to trace

7. Review security monitoring processes

- Evaluate processes for monitoring and maintaining state of security in the system
- Helps to detect security incidents
- How
  - Understand security practices
    - Interview developer, review documentation
    - E.g., routine vulnerability scans,
  - Assess frequency and quality of monitoring
  - Validate security patch policies and procedures

8. Evaluate authentication mechanism

- Ensure app provides mechanism to authenticate users
- Minimum: unique identifier and confidential paswword
- How
  - Review app with developer to verify measures
  - Assess need for additional security e.g. Two-factor authentication in sensitive applications

9. Review authorization mechanism

- Evaluate app authorization mechanism to prevent users from accessing sensitive transactions or data without proper approval
- Ensure each user is given an access level
- How
  - Review app to ensure employees are only given access to accomplish their jobs
  - Verify if possible to check access of each user
    - Transactions and data they can access
    - Level of access i.e., display, update, delete

10. Review the administrator function

- Ensure the existence of administrator function with appropriate controls and functionality
- This account/functionality should be tightly controlled
- How
  - Evaluate the function with developer or app admin
  - Function should be able to
    - Add, delete, modify user access, monitor access of other users
  - Review list of employees who have access

11. Review user access processes

- Ensure access is granted only when there is legitimate business need
- Prevent access beyond scope
- How
  - Review processes for access request and approval
  - Ensure proper documentation of process
  - Select sample of users and verify approval process
  - Verify authorization mechanism

12. Review password controls

- Verify that app has appropriate password controls
- Verify change of default passwords
- Ensure automatic logging off of users
- How
  - Review password policy with app developer or administrator
  - Verify password type, change policy, password composition, max tries, existence of default passwords

Further Reading

- Lecture 9 Reading